

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

17-2
Jc 678 U.S. PTO
09/365446
08/02/99

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1998年 7月31日

出 願 番 号
Application Number:

平成10年特許願第217732号

出 願 人
Applicant (s):

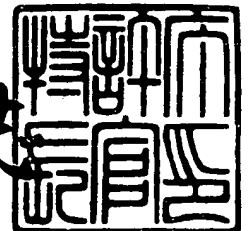
株式会社日立製作所
株式会社日立アドバンスシステムズ
日立京葉エンジニアリング株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 3月26日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



【書類名】 特許願

【整理番号】 HL11836000

【提出日】 平成10年 7月31日

【あて先】 特許庁長官 殿

【国際特許分類】 H04N 7/20
H04L 9/14

【発明の名称】 暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システム

【請求項の数】 22

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所 宇宙技術推進本部内

【氏名】 扇 裕和

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所 宇宙技術推進本部内

【氏名】 高島 英雄

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所 宇宙技術推進本部内

【氏名】 谷口 英宣

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所 宇宙技術推進本部内

【氏名】 高地 宗寿

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所 宇宙技術推進本部内

【氏名】 速水 洋志

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立
アドバンスシステムズ内

【氏名】 浅田 一

【発明者】

【住所又は居所】 千葉県習志野市東習志野 7 丁目 1 番 1 号 日立京葉エン
ジニアリング株式会社内

【氏名】 原▲崎▼ 秀樹

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【特許出願人】

【識別番号】 000153421

【氏名又は名称】 株式会社 日立アドバンスシステムズ

【特許出願人】

【識別番号】 000233217

【氏名又は名称】 日立京葉エンジニアリング株式会社

【代理人】

【識別番号】 100087170

【弁理士】

【氏名又は名称】 富田 和子

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 012014

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

特平 10-217732

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システム

【特許請求の範囲】

【請求項 1】

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側において、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して受信側に伝送すること

を特徴とする暗号化通信方法。

【請求項 2】

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法。

【請求項 3】 請求項 2 に記載の暗号化通信方法において、

予め送信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて受信側に与えること

を特徴とする暗号化通信方法。

【請求項 4】 請求項 2 及び 3 のいずれか一項に記載の暗号化通信方法において、

予め送信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法。

【請求項 5】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 6】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 7】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有

管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 8】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと

、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを前記送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 9】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システム。

【請求項 10】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システム。

【請求項 11】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有

管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 12】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 13】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該発信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該発信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 14】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応し

て前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 15】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システム。

【請求項 16】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システム。

【請求項 17】

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを、送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること
を特徴とする暗号化通信方法。

【請求項 18】

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること
を特徴とする暗号化通信方法。

【請求項 19】 請求項 18 に記載の暗号化通信方法において、

予め受信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて送信側に与えること
を特徴とする暗号化通信方法。

【請求項 20】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

送信側のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子および当該ユーザが運用可能な暗号アルゴリズムの関係が各ユーザについて予め記述されたデータベースを検索して、前記送信側のユーザが運用可能な暗号アルゴリズム、並びに、受信側のユーザが運用可能な暗号アルゴリズムを取得し、

送信側ユーザおよび受信側ユーザに共通して運用可能な暗号アルゴリズムが存在するか否かを判定し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 21】

請求項 20 記載の暗号アルゴリズム共有管理方法において、

前記共通して運用可能な暗号アルゴリズムが存在するとき、当該暗号アルゴリズムを示す情報を前記送信側ユーザに送信し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が不可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項 22】

運用されている第 1 の暗号アルゴリズムを、それと別の第 2 の暗号アルゴリズムに変換するための暗号アルゴリズム変換方法において、

暗号アルゴリズムを変換すべき対象のユーザをキーとして、ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記対象のユーザで運用されている第 1 の暗号アルゴリズム及び第 1 の暗号鍵を取得し、

予め管理用に割り当てられた、前記第 1 の暗号アルゴリズム上で運用される第 1 の管理用秘密鍵で、前記第 1 および第 2 の暗号鍵にそれぞれ署名した第 1 および第 2 の署名データと、予め管理用に割り当てられた前記第 2 暗号アルゴリズム上で運用される第 2 の管理用秘密鍵に対応する第 2 の公開鍵を、前記第 1 の暗号アルゴリズムで暗号化した公開鍵データと、前記第 1 の暗号アルゴリズムで暗号化した第 2 の暗号アルゴリズムと、前記第 2 の管理用秘密鍵に基づいて作成した署名データとを、前記対象のユーザに与えること

を特徴とする暗号アルゴリズム変換方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

暗号化通信における暗号アルゴリズムを他の暗号アルゴリズムに変換するための、暗号化通信方法、暗号アルゴリズム共有管理方法、ネットワーク通信システ

ムに係り、特に、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することに好適な、暗号化通信方法、暗号アルゴリズム共有管理方法、ネットワーク通信システムに関する。

【0002】

【従来の技術】

情報伝達の安全性を確保する手段としては、伝達する情報を暗号化して通信する方法が一般的である。近年、パーソナルコンピュータの性能の向上により、伝達する情報が文書、映像などのデジタル情報の場合、ソフトウェアで暗号化する方法が採用されることも多い。

【0003】

ユーザU〔A〕とユーザU〔B〕とが暗号化通信を行う場合、ユーザU〔A〕は、伝達する情報を暗号化用の鍵で暗号化してデータを送信する。一方、これを受信したユーザU〔B〕は、受信したデータを復号化用の鍵で復号化する。このような暗号化通信は、ユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを共有していることを前提として成り立つ。通常、暗号システムの管理者が暗号アルゴリズムをフロッピーディスクなどの記憶媒体に記録して各ユーザに配布するか、暗号アルゴリズムが実行可能にインストールされた暗号処理機能を有する情報処理装置を配布するなどの方法でアルゴリズムを共有するようにしている。

【0004】

また、暗号アルゴリズムを運用する方法としては、暗号のセキュリティを向上させるため、情報を暗号化するための鍵として、スクランブル鍵を生成するばかりでなく、これとは別にこのスクランブル鍵を暗号化するためのセッション鍵を生成し、ユーザU〔A〕は、ユーザU〔B〕にスクランブル鍵で暗号化した情報と、セッション鍵で暗号化したスクランブル鍵を送付する二重暗号化方式がとられ、暗号化通信が発生するごとに、スクランブル鍵を変更するようにしている。

【0005】

【発明が解決しようとする課題】

(1) 送信側及び受信側で、運用するアルゴリズムが相異なる場合には、暗号化通信を行うことはできない。従って、送信側及び受信側の少なくともいずれかに暗号アルゴリズムを配布する必要がある。

【0006】

ところが、上述した、記憶媒体に記録して各ユーザに配布する方法、暗号アルゴリズムが実行可能にインストールされた暗号機能を有する情報処理装置を配布する方法では、輸送、運送などの手段にたよるため、配布そのものに時間を要する。

【0007】

また、各ユーザに暗号アルゴリズムが配布されると、暗号アルゴリズムをインストールした暗号処理装置と通信機能を有する装置と接続してシステムを構築し、暗号化通信が実施できるか否かの機能確認を行う。この機能確認も、各ユーザ相互に連絡をとりながら実施するため、時間と手間を要する。

【0008】

(2) また、暗号のセキュリティを向上させる方法として、本発明者らの検討によれば、暗号アルゴリズムを定期的に変更して運用することが考えられる。例えば、上述した二重暗号方式におけるセッション鍵の暗号アルゴリズムを定期的に変更するとさらに、セキュリティの向上が期待される。ところが、このためには変更される暗号アルゴリズムを各ユーザに配信する必要がある。この暗号アルゴリズムの配信を前記(1)と同様の配布方法をとったのでは、時間と手間を要し効率が悪くなる。

【0009】

(3) 近年、パーソナルコンピュータなどの情報機器の進歩に伴ない、情報処理速度は年々向上している。暗号アルゴリズムの強度は、このような情報機器をもちいて解読しようと攻撃してきた場合であっても、情報の有効な期限範囲において解読されないような強度である必要がある。

【0010】

ところが、運用する暗号アルゴリズムを常に同一とした場合、情報処理速度の向上により、いつかは解読される危険にさらされることになる。

【0011】

このため、暗号アルゴリズムの強度は、使用される時代の情報機器の情報処理速度に合わせて設定し、強度を高めた暗号アルゴリズムへ変更する必要がある、

(2)と同様効率の良い暗号アルゴリズムの配布方法が必要となる。

【0012】

(4)複数のユーザと、暗号アルゴリズムを運用する鍵を管理する局とが接続される構成として暗号化通信システムを構築することが、本発明者らにより検討されている。ところが、暗号化通信システムに複数の暗号アルゴリズムが混在し、それらの暗号アルゴリズムを定期的に更新するようにすると、このようなシステムには、各ユーザの暗号アルゴリズムを把握し、通信しようとするユーザ相互のアルゴリズムが異なる場合は、同一のアルゴリズムを共有できるようアルゴリズムを配信し、ユーザがアルゴリズムを変更中は、変更中のユーザに関する暗号化通信を停止させるなど、複雑なシステムの運用機能が必要となる。しかし、(1)の暗号アルゴリズムの配布方法をとるとすると、時間と手間を要するばかりでなく、各ユーザの暗号アルゴリズムの状態をリアルタイムに把握するのが難しく、暗号化通信システムが混乱し効率的なシステムの運用が妨げられるおそれがある。

【0013】

(5)暗号アルゴリズムを変更する場合、ユーザが使用する鍵は、変更する暗号アルゴリズムに対応できない可能性がある。

【0014】

共通鍵暗号アルゴリズムから公開鍵暗号アルゴリズムへ変更する場合、または、その逆に公開鍵暗号アルゴリズムから共通鍵暗号アルゴリズムに変更する場合は、ユーザが使用する鍵は変更した暗号アルゴリズムには使用できないという問題を生じる。

【0015】

また、暗号アルゴリズムを強度の高い暗号アルゴリズムに変更した場合、通常は使用する鍵長は長くなる。このため、ユーザが使用する鍵をそのまま変更した暗号アルゴリズムで使用できたとしても、同じ鍵長では、使用しているユーザに対して、暗号強度が増さないという問題を生じる。

【0016】

本発明は、上述のような状況に鑑みてなされたものであり、暗号アルゴリズムの配信を安全に、しかも、それに要する時間と手間を削減した状態で、暗号アルゴリズムを変換することができる、暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システムを提供することを目的とする。

【0017】

また、このような暗号アルゴリズムの変換によって、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することに好適な、暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システムを提供することをも目的とする。

【0018】

【課題を解決するための手段】

前記目的を達成するために、本発明の第1の態様によれば、

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側において、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して受信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【0019】

本発明の第2の態様によれば、

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側で運用される暗号アルゴリズムを、

受信側で運用される暗号アルゴリズムで暗号化して送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法が提供される。

【0020】

本発明の第3の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0021】

本発明の第4の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運

用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0022】

本発明の第5の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0023】

本発明の第6の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを前記送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0024】

本発明の第7の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システムが提供される。

【0025】

本発明の第8の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応

関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システムが提供される。

【0026】

本発明の第9の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0027】

本発明の第10の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0028】

本発明の第11の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該発信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該発信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0029】

本発明の第12の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0030】

本発明の第13の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システムが提供される。

【0031】

本発明の第14の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システムが提供される。

【0032】

本発明の第15の態様によれば、

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを、送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【0033】

本発明の第16の態様によれば、

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【0034】

本発明の第17の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

送信側のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子および当該ユーザが運用可能な暗号アルゴリズムの関係が各ユーザについて予め記述されたデータベースを検索して、前記送信側のユーザが運用可能な暗号アルゴリズム、並びに、受信側のユーザが運用可能な暗号アルゴリズムを取得し、

送信側ユーザおよび受信側ユーザに共通して運用可能な暗号アルゴリズムが存在するか否かを判定し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【0035】

本発明の第18の態様によれば、

運用されている第1の暗号アルゴリズムを、それと別の第2の暗号アルゴリズムに変換するための暗号アルゴリズム変換方法において、

暗号アルゴリズムを変換すべき対象のユーザをキーとして、ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記対象のユーザで運用されている第1の暗号アルゴリズム及び第1の暗号鍵を取得し、

予め管理用に割り当てられた、前記第1の暗号アルゴリズム上で運用される第1の管理用秘密鍵で、前記第1および第2の暗号鍵にそれぞれ署名した第1および第2の署名データと、予め管理用に割り当てられた前記第2の暗号アルゴリズム上で運用される第2の管理用秘密鍵に対応する第2の公開鍵を、前記第1の暗

号アルゴリズムで暗号化した公開鍵データと、前記第1の暗号アルゴリズムで暗号化した第2の暗号アルゴリズムと、前記第2の管理用秘密鍵に基づいて作成した署名データとを、前記対象のユーザに与えること

を特徴とする暗号アルゴリズム変換方法が提供される。

【0036】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態について説明する。

【0037】

まず、本発明を適用したネットワーク通信システムの概略の作用について説明する。

【0038】

本発明を適用した暗号通信システムでは、(1)暗号アルゴリズムを管理する鍵管理局を設置し、当該鍵管理局によって、(2)各ユーザが運用する暗号アルゴリズムの状態を掌握し、(3)各ユーザが使用する暗号アルゴリズムを設定し、(4)各ユーザの使用する暗号アルゴリズムを変換する。以下に、それぞれにおける作用について説明する。

【0039】

(1) まず、暗号アルゴリズムを管理する鍵管理局について説明する。

【0040】

暗号化通信システムに、暗号アルゴリズムを管理する鍵管理局を設置し、各ユーザが使用する暗号アルゴリズム及び更新する暗号アルゴリズムはすべてこの鍵管理局に登録するものとする。

【0041】

(2) 次に、各ユーザの運用する暗号アルゴリズムの状態を掌握する作用について説明する。

【0042】

暗号化通信を行う各ユーザと鍵管理局とは、衛星通信回線または地上回線等の電子通信回線で接続し、鍵管理局は常にこの回線を通して各ユーザの運用する暗号アルゴリズムの状態を掌握し、各ユーザ間で暗号化通信の必要が生じた場合、

当該ユーザが運用する暗号アルゴリズムの運用状態から暗号化通信が可能か判断するものとする。

【0043】

また、鍵管理局は、各ユーザの暗号アルゴリズムの運用状態とともに、当該ユーザの使用する鍵の情報についても掌握しており、当該ユーザの運用する暗号アルゴリズムを変更した場合、当該ユーザの使用する鍵を変更した暗号アルゴリズムに適応できるよう、鍵を変換する情報を作成し、当該ユーザに伝達するものとする。

【0044】

(3) 次に、各ユーザが使用する暗号アルゴリズムを設定する作用について、
(i) 各ユーザ相互に暗号化通信を実施する場合と、(ii) 各ユーザが使用する暗号アルゴリズムの強度を、同等以上の同一系列の暗号アルゴリズムに変換する場合とのそれぞれについて順次説明する。

【0045】

まず、(i) 各ユーザ相互に暗号化通信を実施する場合について説明する。

【0046】

取り得る場合としては、(a) 暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有している場合と、(b) 暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有していない場合とがある。以下にそれぞれの場合に対応した作用について説明する。

【0047】

(a) 暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有している場合

1：鍵管理局は、当該ユーザ相互の暗号化通信が可能と判断し、当該ユーザ相互にこの判断結果を伝達する。

【0048】

2：当該ユーザは、この結果を受けて共有している暗号アルゴリズムにより暗号化通信を実施する。

【0049】

(b) 暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有していない場合

1 : 鍵管理局は、当該ユーザ相互の暗号化通信が不可能と判断する。

【0050】

2 : 鍵管理局は、登録されている暗号アルゴリズムの中からユーザの要求、制約等を考慮し、当該ユーザ相互の暗号化通信に使用する暗号アルゴリズムを設定し、この暗号アルゴリズムを当該ユーザに通信回線を通じて伝達する。

【0051】

また、当該ユーザの使用する鍵を新しく設定した暗号アルゴリズムに適用できるよう変換する必要がある場合は、この鍵変換のための情報を作成し、当該ユーザに通信回線を通じて伝達する。

【0052】

3 : 当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【0053】

次に、(ii) 各ユーザが使用する暗号アルゴリズムの強度を、同等以上の強度の同一系列の暗号アルゴリズムに変換する場合について説明する。暗号アルゴリズムの強度を、同等以上の強度の同一系列の暗号アルゴリズムに変換するためには、例えば、(a) ユーザが使用している暗号アルゴリズムに対して、当該ユーザが同等以上の強度の同一系列の暗号アルゴリズムを提供すること、(b) ユーザが使用しているある暗号アルゴリズムに対して、鍵管理局が暗号アルゴリズム生成装置を所有しており、当該鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを提供することができる。それぞれの作用について以下に説明する。

【0054】

(a) ユーザが使用している暗号アルゴリズムに対して、当該ユーザが同等以上の強度の同一系列の暗号アルゴリズムを提供する場合

1 : ユーザが同等以上の強度の同一系列の暗号アルゴリズムを製作し、当該暗号アルゴリズムを鍵管理局に伝達し、登録する。

【0055】

2：鍵管理局は、前記暗号アルゴリズムの強度を上げる前の暗号アルゴリズムを使用しているユーザを設定し、必要に応じて当該ユーザの使用している鍵変換のための情報を作成し、このユーザに同等以上の強度の同一系列の暗号アルゴリズムと鍵変換のための情報とを送付する。

【0056】

3：当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【0057】

(b) ユーザが使用しているある暗号アルゴリズムに対して、鍵管理局が暗号アルゴリズム生成装置を所有しており、当該鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを提供する場合

1： 鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを作成し、当該暗号アルゴリズムを登録する。

【0058】

2： 鍵管理局は、前記暗号アルゴリズムを変換する前の暗号アルゴリズムを使用しているユーザを設定し、必要に応じて当該ユーザが使用している鍵を変換するための情報を作成し、このユーザに同等以上の強度の同一系列の暗号アルゴリズムと鍵変換のための情報とを送付する。

【0059】

3： 当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【0060】

(4) 次に、各ユーザが使用する暗号アルゴリズムを変換する作用について説明する。

【0061】

1： 鍵管理局は、上述した(3)に従って、各ユーザの変換する暗号アルゴリズム、及び必要に応じ各ユーザの使用する鍵の変換情報を作成する。

【0062】

2: 鍵管理局は、各ユーザの変換する暗号アルゴリズム、及び必要に応じて作成した鍵の変換情報を、各ユーザの運用する変換前の暗号アルゴリズムで暗号化し、各ユーザに通信回線を通じて伝達する。

【0063】

3: 各ユーザは運用している暗号アルゴリズムを使用して、鍵管理局から送付されたデータを復号し変換する暗号アルゴリズム及び鍵の変換情報を取得する。

【0064】

4: 各ユーザは、前記復号したデータをもとに、運用する暗号アルゴリズムと使用する鍵を変更する。

【0065】

5: 各ユーザは変更した暗号アルゴリズムをもちいて、「暗号アルゴリズム変更終了」という文を暗号化し通信回線を介して、鍵管理局に送信する。

【0066】

6: 鍵管理局は、暗号化されて伝達されたデータを復号し、「暗号アルゴリズム変更終了」という文を取得することにより、ユーザの暗号アルゴリズムが変換し、暗号化機能が正常に機能していることを確認する。

【0067】

次に、図1から図5を参照して、本発明の第1の実施の形態について説明する。本実施の形態では、本発明を適用した暗号アルゴリズム変換の概要について説明する。

【0068】

まず、図1を参照して、本発明の適用対象となるネットワーク通信システムについて説明する。ここでは、ユーザが使用する複数のパーソナルコンピュータ（情報処理装置）100、200と鍵管理局400とが接続された構成例について説明する。

【0069】

本システムに運用される暗号アルゴリズムを、 $A[1] \sim A[n]$ 、 $B[1]$

～B[m]とし、これらの暗号アルゴリズムを鍵管理局が管理している。暗号アルゴリズムのA[1]～A[n]は、同一のA系列の暗号強度が同一または異なる暗号アルゴリズムであり、暗号強度が同等以上の同一系列の暗号アルゴリズムに変更することによるセキュリティの更新を鍵管理局が実施している。

【0070】

暗号アルゴリズムA[1]を運用するユーザのユーザIDをU[A₁, 1]～U[A₁, N₁]、暗号アルゴリズムA[2]を運用するユーザのユーザIDをU[A₂, 1]～U[A₂, N₂]、…、暗号アルゴリズムA[n]を運用するユーザのユーザIDをU[A_n, 1]～U[A_n, N_n]とし、暗号アルゴリズムB[1]を運用するユーザのユーザIDをU[B₁, 1]～U[B₁, M₁]、暗号アルゴリズムB[2]を運用するユーザのユーザIDをU[B₂, 1]～U[B₂, M₂]、…、暗号アルゴリズムB[m]を運用するユーザのユーザIDをU[B_n, 1]～U[B_n, M_m]とし、鍵管理局は各ユーザの運用する暗号アルゴリズムとユーザIDを対応させて管理している。

【0071】

図1において、A系列に属する暗号アルゴリズムのうちの1つ（以下、単に暗号アルゴリズムAという）を運用するユーザが使用するパーソナルコンピュータ100と、B系列に属する暗号アルゴリズムのうちの1つ（以下、単に暗号アルゴリズムBという）を運用するユーザが使用するパーソナルコンピュータ200と、鍵管理用ワークステーション500を備える鍵管理局400とがネットワークに接続されている。

【0072】

このネットワーク通信システムでは、暗号化通信、暗号アルゴリズム変換等は、各ユーザが使用する情報処理装置などのパーソナルコンピュータ100、200及び、鍵管理用ワークステーション500のソフト処理によって実施される。

【0073】

図22は、複数の暗号アルゴリズムが存在するネットワーク通信システムの図1とは別の形態を示している。この形態のネットワーク通信システムでは、ネットワーク通信システムに、暗号アルゴリズムとして、アルゴリズムA、アルゴリ

ズムB、アルゴリズムC、アルゴリズムDと、4つの暗号アルゴリズムが混在している。

【0074】

通常、使用する暗号アルゴリズムは、ユーザが選択して定める。

【0075】

暗号アルゴリズムの性質から、ユーザが使用したくないものも存在する。

【0076】

図22に示されるネットワーク通信システムでは、前記4つの暗号アルゴリズム、A、B、CおよびDが使用されている。なお、本図において、暗号アルゴリズムAを使用するユーザの範囲を実線で示し、暗号アルゴリズムBを使用するユーザの範囲を一点鎖線で示し、暗号アルゴリズムCを使用するユーザの範囲を二点鎖線で示し、暗号アルゴリズムDを使用するユーザの範囲を破線で示している。

【0077】

各暗号アルゴリズムの使用範囲が、重なっている部分のユーザは、複数の暗号アルゴリズムを使用することができる。

【0078】

鍵管理局は、各暗号アルゴリズムに対して、その暗号アルゴリズムを使用可能なユーザをデータベースに格納している。

【0079】

各ユーザ間で、暗号化通信要求が発生した場合、鍵管理用ワークステーションは、前記データベースに基づき、送信側及び受信側それぞれの暗号アルゴリズムの運用状態を把握する。

【0080】

送信側及び受信側で同一の暗号アルゴリズムを共有している場合は、両者の暗号化通信を続行させる。

【0081】

同一の暗号アルゴリズムを共有していない場合、前記データベースに基づき、送信側及び受信側ユーザに同一の暗号アルゴリズムを持たせることが可能か否か

を判断する。

【0082】

共有させることができない場合は、両者に暗号化通信ができないことを連絡する。

【0083】

ユーザ相互に暗号アルゴリズムを共有できるかどうかは、ユーザの都合によって定まるものである。

【0084】

各暗号アルゴリズムを使用するユーザの範囲は、ユーザの都合によって変化する。

【0085】

鍵管理用ワークステーションは、ユーザ等の連絡により各暗号アルゴリズムを使用するユーザを示すデータベースに格納される情報を変更するものとする。

【0086】

次に、図2を参照して、本ネットワーク通信システムにおける各情報処理装置（パーソナルコンピュータ、鍵管理用ワークステーション）が備えるソフト処理機能について説明する。

【0087】

図2において、パーソナルコンピュータ100及び200とが接続されてネットワークが構成されている。以下、パーソナルコンピュータ100が送信側ユーザに使用され、パーソナルコンピュータ200が受信側ユーザに使用される場合について説明する。なお、パーソナルコンピュータ100及び200は同様に構成されるので、これらは、送信側、受信側のいずれにも使用することが可能であることは勿論である。また、鍵管理用ワークステーション500が、少なくとも送信側ユーザに使用されるパーソナルコンピュータ100と接続されている。

【0088】

前記送信側（受信側）ユーザが使用するパーソナルコンピュータ100（200）は、鍵構成管理機能110（210）と、暗号アルゴリズム管理機能120（220）と、スクランブル機能130（230）と、デスクランブル機能14

0(240)と、暗号化通信管理機能150(250)とを備え、鍵構成管理データベース180(280)と、暗号アルゴリズムデータベース190(290)とをアクセス可能に接続されている。

【0089】

なお、これらのデータベースは、パーソナルコンピュータ100, 200と別個に備えられてもよいし、パーソナルコンピュータ100, 200と一体に構成されてもよい。また、前記データベースは、複数のパーソナルコンピュータで共有されていてもよい。

【0090】

前記鍵管理用ワークステーション500は、スクランブル機能530と、デスクランブル機能540と、暗号化通信管理機能550と、暗号アルゴリズム生成機能595と、ネットワーク暗号管理機能560と、ネットワーク鍵管理機能570とを備え、ネットワーク暗号アルゴリズム管理データベース590と、ネットワーク鍵管理データベースとにアクセス可能に接続される。なお、これらのデータベースは、鍵管理用ワークステーション500と別個に設置されてもよいし、鍵管理用ワークステーション500と一体に構成されてもよい。

【0091】

次に、同じく図2を参照して、鍵管理用ワークステーション500の機能について説明する。

【0092】

ネットワーク暗号アルゴリズム管理DB590には、各ユーザのユーザIDと暗号アルゴリズムとを対応させて登録している。

【0093】

ネットワーク暗号アルゴリズム管理機能570は、前記2組のデータに関するDBを管理しており、各ユーザの使用する暗号アルゴリズムの、登録、更新、削除を実施している。

【0094】

暗号アルゴリズム生成機能595は、A系列の暗号アルゴリズムを生成する機能を有している。

【0095】

暗号アルゴリズムの暗号強度は、運用する鍵の鍵長が長くなると暗号解読がより困難になり暗号強度が増加してセキュリティを改善することができる。

【0096】

また、同じ鍵長の暗号アルゴリズムでも定期的に運用する暗号アルゴリズムを変更すれば、暗号攻撃の期間を限定することができ、通信上のセキュリティを改善することができる。

【0097】

暗号アルゴリズム生成機能595は、使用する鍵長が同じものか、または、鍵長が長くなるような、A系列における相異なる暗号アルゴリズムを生成している。

【0098】

ネットワーク鍵構成管理機能570は、本システムで運用される鍵を管理し、ネットワーク鍵構成管理DBにユーザの使用する鍵情報を格納している。

【0099】

スクランブル機能530は、鍵管理局400（図1参照）がユーザに送信するデータを暗号化する機能であり、デスクランブル機能540は、鍵管理局400（図1参照）がユーザから受信した暗号化されたデータを復号するための機能である。

【0100】

ネットワーク鍵管理機能570は、暗号化、復号化に使用する鍵の管理を実施しており、鍵構成管理DB180、280に運用する暗号アルゴリズムに対応させて各ユーザが使用する鍵に関する情報を格納している。

【0101】

次に、前記ユーザが使用する情報処理装置などのパーソナルコンピュータ100（200）のソフト機能について説明する。

【0102】

暗号アルゴリズム管理機能120（220）は、ユーザが運用する暗号アルゴリズムを管理している。

【0103】

運用する暗号アルゴリズムは、鍵管理用ワークステーション500の指示により、暗号アルゴリズムを変換する。暗号アルゴリズム管理DBには、鍵管理局400（図1参照）より配布される暗号アルゴリズムを格納している。

【0104】

スクランブル機能130（230）は、ユーザが送信するデータを暗号化する機能であり、デスクランブル機能140（240）は、ユーザが受信した暗号化されたデータを復号する機能である。

【0105】

鍵構成管理機能110（210）は、暗号化、復号化に使用する鍵の管理を実施しており、鍵構成管理DB180（280）に運用する暗号アルゴリズムに対応させて鍵を格納している。

【0106】

次に、図3を参照して、前記鍵管理用ワークステーションからアクセスされるデータベースに格納される情報の内容について説明する。

【0107】

図3の（a）において、ネットワーク暗号アルゴリズム管理データベースには、ユーザを識別するためのユーザIDと、当該ユーザが運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンとの対応関係が記述され、さらのその更新日時が記述された情報、及び、鍵管理局を識別するための鍵管理局IDと、当該鍵管理局が運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンとの対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【0108】

図3の（b）において、ネットワーク鍵管理データベースには、ユーザを識別するためのユーザIDと、当該ユーザが運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、運用される暗号鍵を示す鍵情報との対応関係が記述され、さらのその更新日時が記述された情報、及び、鍵管理局を識別するための鍵管理局IDと、当該鍵管理局が運用する暗号アルゴリズムの

暗号アルゴリズム名及び暗号アルゴリズムバージョンと、運用される暗号鍵を示す鍵情報との対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【0109】

次に、図4を参照して、前記ユーザが使用するパーソナルコンピュータからアクセスされるデータベースに格納される情報の内容について説明する。

【0110】

図4の(a)において、暗号アルゴリズム管理データベースには、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンの対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【0111】

図4の(b)において、鍵管理データベースには、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、ユーザの暗号鍵を示すユーザ鍵情報との対応関係が記述され、さらのその更新日時が記述された情報、及び、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、鍵管理局の暗号鍵を示す鍵管理局の鍵情報との対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【0112】

次に、図7を参照して、送信、受信双方のユーザが同一の暗号アルゴリズム（ここでは、共通鍵暗号が運用されているものとする）を共有している場合の暗号化通信の概要について説明する。この場合、送信側ユーザをAとし、受信側ユーザをBとし、これらの間で伝送される送信データをMとする。

【0113】

ユーザU[A]は、鍵管理用ワークステーション500に対してユーザU[B]を指定し、暗号通信に用いるセッション鍵発行要求を行う。

【0114】

鍵管理用ワークステーション500は、この要求を受け、ユーザU[B]と暗号通信を可能とするセッション鍵をユーザU[B]に発行する。

【0115】

ユーザU〔A〕は、このセッション鍵の発行を受けると、自分が使用するパーソナルコンピュータのスクランブル機能130と組み合わせて、データMを暗号化し、暗号文としてユーザU〔B〕に送付する。

【0116】

ユーザU〔B〕は、ユーザU〔A〕と同じ暗号アルゴリズムを暗号アルゴリズムDB190に格納している。これより、ユーザU〔B〕は、ユーザU〔A〕から送付された、暗号文をデスクランブル機能140より復号しデータMを取得する。

【0117】

一方、送信、受信双方のユーザで、運用される暗号アルゴリズムが相違する場合として、例えば、運用する暗号アルゴリズムA〔1〕～A〔n〕，B〔1〕～B〔m〕が、共通鍵暗号アルゴリズム、公開鍵暗号アルゴリズムの方式が相異なる複数の暗号アルゴリズムが混在していることがある。

【0118】

ユーザU〔A〕がユーザU〔B〕に暗号化通信を実施する場合、双方のユーザが同一の暗号アルゴリズムを共有している場合は、そのまま暗号化通信を実施できるが、同一の暗号アルゴリズムを共有していない場合は、ユーザが所有する暗号アルゴリズムを変換し双方のユーザに同一の暗号アルゴリズムを共有させて、暗号化通信を実施する。

【0119】

この暗号アルゴリズムの変換は、ユーザの所有する暗号アルゴリズムの状態に応じて、下記に示すような暗号アルゴリズム変換を実施する。

【0120】

(1) 同一系列の暗号アルゴリズムは、バージョン番号で管理し、同じ暗号強度を有する他の暗号アルゴリズム、または、異なる暗号強度を有する他の暗号強度を暗号アルゴリズムへ変換する。

【0121】

(2) 共通鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する。

【0122】

(3) 公開鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへ変換する。

【0123】

(4) 共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへ変換する。

【0124】

(5) 公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する。

【0125】

ここで言う、暗号アルゴリズムとは、一連のデータの変換手順を指すものである。

【0126】

暗号化とは、データの変換を意味し、復号とは変換されたデータの逆変換を意味している。

【0127】

例えば、Kを二進法のデータ列とし、Mを別の二進法のデータ列とする。

【0128】

このKが定める以下の π 関数を考える。

【0129】

$$\pi(M) = M \text{ xor } K$$

ここで、xorは、MとKとの排他的論理和を示している。

【0130】

$\pi(M)$ により、データMは、変換された。この変換されたデータに対して、

$$\pi(M) \text{ xor } K$$

を求めると、

$$\begin{aligned} \pi(M) \text{ xor } K &= (M \text{ xor } K) \text{ xor } K \\ &= M \text{ xor } (K \text{ xor } K) \\ &= M \end{aligned}$$

となり、変換されたデータ $\pi(M)$ からデータMが逆変換された。

【0131】

この π 関数のような、データの変換及び逆変換の手順を暗号アルゴリズムと呼

ぶ。

【0132】

次に、N個のデータの組 $\{K_1, K_2, K_3, \dots, K_N\}$ を考え、i 番目のデータ K_i に対応する関数を π_i とする。このN個の π 関数から次の2組の関数 f, g を考える。

【0133】

$$f = \pi_1 \circ \pi_2 \circ \pi_3 \circ \dots \circ \pi_N$$

$$g = \pi_N \circ \pi_{N-1} \circ \pi_{N-2} \circ \dots \circ \pi_1$$

この2組の関数 f, g は、このn個の π 関数の演算をN回繰り返したものである。

【0134】

従って、 $f(M), g(M)$ は、それぞれデータMの変換手順を示し、変換されたデータ $f(M)$ は、関数 g によって逆変換され、データMが導出される。

【0135】

このため、関数 f, g は、1つの暗号アルゴリズムと考えることができ、関数 f は、データの暗号化に対応し、関数 g は、データの復号化に対応するものと考えられる。

【0136】

N個の π 関数の演算順序や、パラメータ K_i の値を変更すると、別の暗号アルゴリズムが得られる。

【0137】

前述の暗号アルゴリズム変換で述べた同一系列の暗号アルゴリズムとは、このようにデータ変換の一部の順序を変更したり、使用するパラメータの値を変えて組み立てた暗号アルゴリズムを指すものである。同一系列の暗号アルゴリズムのことを、以降、バージョンが異なる暗号アルゴリズムと呼ぶことにする。

【0138】

このような、暗号アルゴリズム変換を実施する場合、ユーザが所有する鍵も、変換した暗号アルゴリズムにあわせて変換を実施する。

【0139】

次に、図5を参照して、本発明を適用した、ネットワーク通信で運用する暗号アルゴリズム変換の概要について説明する。

【0140】

ここで、送信側ユーザを $U[A]$ とし、 $U[A]$ が運用している暗号アルゴリズムを暗号アルゴリズム $EANG$ とする。一方、受信側ユーザを $U[B]$ とし、 $U[B]$ が運用している暗号アルゴリズムを暗号アルゴリズム EBF とする。

【0141】

鍵管理用ワークステーション500のネットワーク暗号アルゴリズム管理DB590には、暗号アルゴリズム $EANG$ をユーザ $U[A]$ のユーザIDと対応させ、暗号アルゴリズム EBF をユーザ $U[B]$ のユーザIDと対応させて、格納している。

【0142】

また、暗号アルゴリズム $EANG$ で鍵管理用ワークステーション500が、ユーザ $U[A]$ と暗号化通信を実施するための鍵を K_A とし、暗号アルゴリズム EBF で鍵管理用ワークステーション500が、ユーザ $U[B]$ と暗号化通信を実施するための鍵を K_B とする。

【0143】

ユーザ $U[A]$ の鍵構成管理DB（図示せず）には、鍵 K_A が格納されており、ユーザ $U[B]$ の鍵構成管理DB180には、鍵 K_B が格納されており、鍵管理用ワークステーション500のネットワーク鍵管理DB580には、ユーザ $U[A]$ のユーザIDと対応させて鍵 K_A を格納し、ユーザ $U[B]$ のユーザIDと対応させて鍵 K_B を格納している。

【0144】

以上の環境のもとで、ユーザ $U[A]$ がユーザ $U[B]$ に暗号化通信を実施する場合を例にして、本ネットワーク通信システムで運用する暗号アルゴリズム変換について概略を説明する。

【0145】

1： ユーザ $U[A]$ は、暗号化通信管理機能150より、送信相手をユーザ

U [B] のユーザIDで指定し<セッション鍵発行要求>を鍵管理ワークステーション500の暗号化通信管理機能550に送付する。

【0146】

2: <セッション鍵発行要求>は、鍵管理ワークステーション500のネットワーク暗号アルゴリズム管理機能560に送付される。ネットワーク暗号アルゴリズム管理機能560は、ユーザU [A] のユーザIDと、ユーザU [B] のユーザIDとに基づいて、ネットワーク暗号アルゴリズムDB590の検索を行う。

【0147】

ユーザU [A] が運用する暗号アルゴリズムは暗号アルゴリズムEANGであり、ユーザU [B] の暗号アルゴリズムは暗号アルゴリズムEBFである。このため、同一の暗号アルゴリズムを共有していないと判断し、この結果を暗号化通信管理機能550に送付する。

【0148】

3: この結果を受けて、暗号化通信管理機能550は、ユーザU [B] の暗号アルゴリズムをEBFからEANGへの変換動作を始める。

【0149】

まず、暗号アルゴリズムEANGでユーザU [B] と暗号化通信を実施するための鍵 L_B を生成し、平文データMDを<デスクランブル機能確認終了>と定める。

【0150】

次に、暗号アルゴリズムEANG及び鍵 L_B を、暗号アルゴリズムEBF及び鍵 K_B でそれぞれ暗号化して、暗号文 $EBF_{KB}(EANG)$ 及び $EBF_{KB}(L_B)$ を作成する。

【0151】

さらに、平文データMDを暗号アルゴリズムEANG及び鍵 L_B で暗号化して、暗号文 $EANG_{LB}(MD)$ を作成する。前記3組の暗号文は、鍵管理ワークステーション500のスクランブル機能530により作成される。

【0152】

この3組の暗号文を<暗号アルゴリズム更新要求>として、ユーザU〔B〕に配信する。

【0153】

4： この3組の暗号文、 $E B F_{KB} (E A N G)$ 、 $E B F_{KB} (L_B)$ 及び $E A N G_{LB} (MD)$ を受け取ったユーザU〔B〕は、デスクランブル機能140によりこれらの暗号文を復号する。

【0154】

まず、鍵構成管理DB180に格納されている鍵 K_B より、暗号文 $E B F_{KB} (E A N G)$ と暗号文 $E B F_{KB} (L_B)$ を復号し、暗号アルゴリズムEANG、及び鍵 L_B を取得する。

【0155】

暗号アルゴリズム管理機能120は、取得した暗号アルゴリズムEANGを暗号アルゴリズムDB190に格納するとともに、暗号アルゴリズムの運用状態を暗号アルゴリズムEBFから、暗号アルゴリズムEANGに更新する。また、鍵構成管理機能110は、取得した鍵 L_B を鍵構成管理DB180に格納する。

【0156】

このようにして、暗号アルゴリズム及び鍵が更新された。

【0157】

次に、更新された暗号アルゴリズムEANG及び鍵 L_B を用いて、暗号文 $E A N G_{LB} (MD)$ を復号し、平文データMDを取得する。取得した平文データMDが<デスクランブル機能確認終了>となっていることを確認し、変換した暗号アルゴリズムEANGによるデスクランブル機能140が正常に動作することを確認する。

【0158】

5： 次に、平文データMSを<スクランブル機能確認終了>とし、スクランブル機能130を動作させ暗号アルゴリズムEANG及び鍵 L_B を用いて暗号化し、暗号文 $E A N G_{LB} (MS)$ を作成する。

【0159】

この作成した暗号文を<暗号アルゴリズム更新報告>として、鍵管理用ワークステーション500に配信する。

【0160】

6: <暗号アルゴリズム更新報告>を受信した鍵管理用ワークステーションは、暗号アルゴリズムEANG及び鍵 L_B を用いて復号化し、平文データMSを取得する。取得した平文データMSが<スクランブル機能確認終了>となっていることを確認し、ユーザU[B]の変換した暗号アルゴリズムEANGによるスクランブル機能130が正常に動作することを確認する。これにより、暗号アルゴリズム変換と、暗号化、復号化を実施するスクランブル機能130、デスクランブル機能140とが正常に動作することが確認され、暗号アルゴリズム変換を終了する。

【0161】

7: 以上の手順により、ユーザU[A]とユーザU[B]とは、同一の暗号アルゴリズムEANGを共有することが可能となった。これより、ユーザU[A]とユーザU[B]との暗号化通信を再開し、鍵管理用ワークステーションはユーザU[A]にアルゴリズムEANGに基づいて<セッション鍵発行>を実施する。

【0162】

以上、暗号アルゴリズムの暗号化による配信と、運用する鍵の変換及び、変換した暗号アルゴリズムの動作確認の手順について説明した。

【0163】

以下に、アルゴリズム変換の詳細について説明する。ここでは、運用される暗号が公開鍵暗号か共通鍵暗号かについて着目し、暗号化通信システムが共通鍵暗号で構成されている場合の暗号アルゴリズム変換（本発明の第2の実施の形態）について説明し、次に、暗号化通信システムが公開鍵暗号で構成されている場合の暗号アルゴリズム変換（本発明の第3の実施の形態）について説明する。なお、これらの実施の形態において、基本的な構成は、上述した第1の実施の形態と同様であるので、以下の説明では、その相違点を中心にして、それぞれの場合の

暗号アルゴリズム変換の詳細について説明する。

【0164】

まず、図6から図10を参照して、本発明の第2の実施の形態について説明する。ここでは、共通鍵暗号で構成されている暗号化通信システムにおける暗号アルゴリズム変換について説明する。すなわち、図1の暗号化通信システムにおいて、運用される暗号アルゴリズム $A[1] \sim A[n]$ 及び $B[1] \sim B[m]$ がすべて共通鍵暗号アルゴリズムである場合の暗号アルゴリズム変換について説明する。

【0165】

図5及び図7を参照して、共通鍵暗号アルゴリズムによる暗号化通信について説明する。

【0166】

暗号化通信を行う前提条件とし、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザIDと、マスター鍵としての秘密鍵とが割り当てられており、鍵管理用ワークステーションのネットワーク鍵構成DBに、ユーザに割り当てたマスター鍵をユーザIDと対応させて登録し管理しているものとする。同様に鍵管理局自身にもマスター鍵としての秘密鍵 P_{CID} が割り当てられているものとする。

【0167】

本実施の形態では、データの暗号化に用いるスクランブル鍵 k_s の暗号アルゴリズムと、デスクランブル鍵 K_D の配送に用いるセッション鍵の暗号アルゴリズムとを、異なった暗号アルゴリズムとする二重暗号化方式を取っており、同一の暗号アルゴリズムを使用する場合とくらべてセキュリティの向上を図っている。本実施例では、セッション鍵とマスター鍵を運用する暗号アルゴリズムは、同一の暗号アルゴリズムを使用することとしている。

【0168】

以下、ユーザ $U[A]$ からユーザ $U[B]$ に暗号化通信を行う場合を例にして、暗号化通信の内容について説明する。

【0169】

(1) ユーザU〔A〕からユーザU〔B〕に暗号化通信を行う場合、ユーザU〔A〕は鍵管理局に、セッション鍵発行要求を行う。ここで、ユーザU〔A〕は、送信側ユーザとし、ユーザU〔B〕は、受信側ユーザとする。このセッション鍵発行要求を受けて、鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能は、ネットワーク暗号アルゴリズムDBの検索を行い、ユーザU〔A〕とユーザU〔B〕とが使用している暗号アルゴリズムが同一かどうかの判断を行う。

【0170】

(2) ユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを使用していると判断したとき、鍵管理用ワークステーションのネットワーク鍵管理機能は、その暗号アルゴリズムでセッション鍵 P_T を生成する。次に、送信側のユーザのマスター鍵 P_{ID} 、受信側のユーザのマスター鍵 P_{YID} をネットワーク鍵管理DBより取り出し、セッション鍵 P_T を平文として暗号化を行い、暗号文 $E_{PID}(P_T)$ 、 $E_{PYID}(P_T)$ を作成する。この暗号文を送信側ユーザの使用するパーソナルコンピュータなどの情報処理装置に送付する。

【0171】

(3) 送信側のユーザが使用するパーソナルコンピュータでは、管理しているユーザのマスター鍵 P_{ID} を鍵構成管理DBより取り出し、この鍵を用いて、暗号化されて送付されたセッション鍵を復号し、セッション鍵 P_T を取得する。

【0172】

(4) 一方、ユーザが入力したデータMを受け取り、このデータMを暗号化するためのスクランブル鍵 k_S 、復号化するためのデスクランブル鍵 K_D を生成する。

【0173】

(5) 次に、ユーザが入力したデータMをスクランブル鍵 k_S で暗号化し、暗号文 $E_{k_S}(M)$ を作成し、同様にデスクランブル鍵 K_D をセッション鍵 P_T で暗号化し、暗号文 $E_{P_T}(K_D)$ を作成する。この作成した2組の暗号文と、送付された暗号文 $E_{PYID}(P_T)$ とを送信先相手のユーザの使用するパーソナルコンピュ

ータなどの情報処理装置に送信する。

【0174】

(6) 送信先相手ユーザ側のパーソナルコンピュータは、このユーザのマスター鍵 P_{YID} を鍵構成管理DBより取り出し、この鍵を用いて送付された暗号化セッション鍵 $E_{PYID}(P_T)$ を復号し、セッション鍵 P_T を取得する。次に送付された暗号化デスクランブル鍵 $E_{PT}(K_D)$ を取得したセッション鍵 P_T を用いて復号し、デスクランブル鍵 K_D を取得する。

【0175】

最後に、このデスクランブル鍵 K_D を用いて送付されたデータの暗号文 $E_{ks}(M)$ を復号し、データ M を取得する。

【0176】

鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能がユーザ $U[A]$ とユーザ $U[B]$ とが同一の暗号アルゴリズムを使用していないと判断すると、ユーザ $U[B]$ の暗号アルゴリズムの変換を実施し、ユーザ $U[A]$ とユーザ $U[B]$ とが同一の暗号アルゴリズムを運用できるようにする。

【0177】

次に、図6及び図8、9を参照して、本実施の形態における暗号アルゴリズム変換の手順について説明する。

【0178】

(1) ネットワーク暗号アルゴリズム管理機能は、送信側のユーザから、送信側ユーザのユーザIDと送信先相手ユーザのユーザIDとを付加したセッション鍵発行要求を受けると、送付されたユーザIDをキーとして、ネットワーク暗号アルゴリズムDBの検索を実施し、送信側ユーザと送信先相手ユーザの運用する暗号アルゴリズムの状態を把握する。図7に示すように暗号化通信システムは共通鍵暗号による二重暗号方式をとっており、データの暗号化に用いる暗号アルゴリズムと、セッション鍵を運用する暗号アルゴリズムとの二種類の暗号アルゴリズムを用いている。送信側ユーザと送信先相手ユーザとが運用する二種類の暗号アルゴリズムが一致しないと、両者の間で暗号化通信を実施することはできない。

【0179】

ネットワーク暗号アルゴリズムDBを検索の結果、一致しない場合、送信側ユーザの運用する暗号アルゴリズムEANGを取り出す。取り出した暗号アルゴリズムには、データの暗号化に用いるものか、セッション鍵の運用に用いるかの識別子を付加するものとする。当然、二種類の暗号アルゴリズムが一致しなければ、二種類の暗号アルゴリズムを取り出すことになる。

【0180】

送信先相手ユーザの運用している暗号アルゴリズムをEBFとすると、この暗号アルゴリズムEBFから取り出した暗号アルゴリズムEANGに暗号アルゴリズムを変換させることになる。

【0181】

(2) 鍵管理用ワークステーションのネットワーク鍵管理機能は、変換前の暗号アルゴリズムEBFでセッション鍵 P_{TA} を生成し、変換後の暗号アルゴリズムEANGでセッション鍵 P_{TB} を生成する。セッション鍵を運用するアルゴリズムに変更がなければ、 P_{TA} 及び P_{TB} は同一である。次に、送信先相手ユーザのユーザIDキーとして、ネットワーク鍵管理DBを検索し、送信先相手ユーザのマスター鍵 P_{YID} を取り出す。

【0182】

暗号アルゴリズムを変換した場合、暗号化通信に使用する鍵の鍵長すなわちビット数は、長くなったり、短くなったりする。従って、このような場合には、暗号鍵の鍵長の変更を暗号アルゴリズムの変換と併せて行うことが要求される。

【0183】

図10を参照して、暗号アルゴリズムの変換に伴う、暗号鍵の変換について説明する。

【0184】

鍵のビット数が短くなる場合は、図10の(a)に示すように、送信先相手ユーザのマスター鍵 P_{YID} 及び、鍵管理局自身のマスター鍵 P_{CID} の後ろの冗長分のビット数を削除し、新しく送信先相手ユーザのマスター鍵 P_{YIDC} 及び、鍵管理局自身のマスター鍵 P_{CIDC} とする。

【0185】

一方、鍵のビット数が長くなる場合は、図10の(b)に示すように、不足分のビット数に合わせて乱数YR, CRを生成し、 P_{YID} に乱数YRをつなげて、新しく送信先相手ユーザのマスター鍵 P_{YIDC} ($P_{YIDC} = P_{YID} \parallel YR$)とし、 P_{CID} に乱数CRをつなげて新しくネットワーク鍵管理用ワークステーション自身のマスター鍵 P_{CIDC} ($C_{CIDC} = C_{CID} \parallel CR$)とする。

【0186】

ここで、新しく更新したユーザのマスター鍵 P_{YIDC} , P_{CIDC} は、ほかのユーザのマスター鍵と同一の可能性があるため、ネットワーク鍵管理DBを検索し、同一のマスター鍵のユーザがないことを確認し、また、同一のマスター鍵のユーザが存在する場合は、必要な鍵長で新しく生成するものとする。

【0187】

(3) 変換前の暗号アルゴリズムEBFを使用して以下の暗号文を作成する。

【0188】

1: 変換前の暗号アルゴリズムEBFとマスター鍵 P_{YID} でセッション鍵 P_{TA} を暗号化し、暗号文 $EBF_{PYID}(P_{TA})$ を作成する。

【0189】

2: 変換前の暗号アルゴリズムEBFとセッション鍵 P_{TA} で暗号アルゴリズムEANGを暗号化し、暗号文 $EBF_{PTA}(EANG)$ を作成する。

【0190】

3: 変換前の暗号アルゴリズムEBFとセッション鍵 P_{TA} で変換後の送信先相手ユーザのマスター鍵 P_{YIDC} を暗号化し、暗号文 $EBF_{PTA}(P_{YIDC})$ を作成する。当然、送信先相手ユーザのマスター鍵に変更がなければ、この暗号文は作成しない。

【0191】

(4) 変換後の暗号アルゴリズムEANGを使用して以下の暗号文を作成する。

【0192】

1: 変換後の暗号アルゴリズムEANGと、変換後の送信先相手ユーザのマ

スター鍵 P_{YIDC} とで変換後の暗号アルゴリズムで運用するセッション鍵 P_{TB} を暗号化し暗号文 $EANG_{PYIDC}(P_{TB})$ を作成する。

【0193】

当然、セッション鍵を運用する暗号アルゴリズムに変更がなければ、この暗号文は、 $EBF_{PYID}(P_{TA})$ と同じである。

【0194】

2： 変換後の暗号アルゴリズム $EANG$ と変換後の鍵管理用ワークステーション自身のマスター鍵 P_{CIDC} で変換後の暗号アルゴリズムで運用するセッション鍵 P_{TB} を暗号化し暗号文 $EANG_{PCIDC}(P_{TB})$ を作成する。

【0195】

当然、セッション鍵を運用する暗号アルゴリズムに変更がなければ、この暗号文は、変換前の暗号アルゴリズム EBF と変換前の鍵管理用ワークステーション自身のマスター鍵 P_{CID} で変換前の暗号アルゴリズムで運用するセッション鍵 P_{TA} を暗号化して作成する暗号文 $EBF_{PCID}(P_{TA})$ と同じものになる。

【0196】

3： 平文データ MD を<アルゴリズム変換後のデスクランブル機能確認終了>とする。

【0197】

変換後の暗号アルゴリズム $EANG$ でこの平文データ MD を暗号化するためのスクランブル鍵 k_{SC} 、復号化するためのデスクランブル鍵 K_{DC} を生成する。

【0198】

次に、データ MD をスクランブル鍵 k_{SC} で暗号化し、暗号文 $E_{kSC}(MD)$ を作成し、同様にデスクランブル鍵 K_{DC} を変換後の暗号アルゴリズムで運用するセッション鍵 P_{TB} で暗号化し、暗号文 $EANG_{PTB}(K_{DC})$ を作成する。

【0199】

(5) 前記(3)項で作成した3組の暗号文 $EBF_{PYID}(P_{TA})$ 、 $EBF_{PTA}(EANG)$ 及び $EBF_{PTA}(P_{YIDC})$ と、前記(4)で作成した4組の暗号文 $EANG_{PYIDC}(P_{TB})$ 、 $EANG_{PCIDC}(P_{TB})$ 、 $E_{kSC}(MD)$ 及び $EANG_{PTB}(K_{DC})$ とを<暗号アルゴリズム変換要求>として、送信先相手ユーザに送付

する。ここで、前記（３）項で作成した３組の暗号文は、送信先相手ユーザの暗号アルゴリズムを変換するための情報であり、前記（４）項で作成した４組の暗号文は、暗号アルゴリズムを変換後、変換した暗号アルゴリズムが正常に機能するか確認するための情報である。

【0200】

（６）送信先相手ユーザの暗号アルゴリズムの変換、及びマスター鍵の更新
送信先相手ユーザは、暗号アルゴリズムとしてEBFを運用しており、マスター鍵として P_{YID} を所有している。鍵管理用ワークステーションより送付された暗号文から、

１： マスター鍵として P_{YID} を用いて、暗号文 $EBF_{PYID}(P_{TA})$ を復号し、セッション鍵 P_{TA} を取得する。

【0201】

２： セッション鍵 P_{TA} を用いて暗号文 $EBF_{PTA}(EANG)$ を復号し、暗号アルゴリズムEANGを取得する。

【0202】

３： セッション鍵 P_{TA} を用いて暗号文 $EBF_{PTA}(P_{YIDC})$ を復号し、マスター鍵 P_{YIDC} を取得する。

【0203】

以上のようにして、送信先相手ユーザは、暗号アルゴリズムEANGとマスター鍵 P_{YIDC} とを取得した。これより、取得した暗号アルゴリズムEANGを暗号アルゴリズム管理DBに登録するとともに、暗号アルゴリズム管理機能により運用する暗号アルゴリズムをEBFからEANGに変換する。

【0204】

送信先相手ユーザのマスター鍵が変更になる場合は、鍵構成管理機能によりマスター鍵を P_{YID} から P_{YIDC} に更新する。

【0205】

（７）送信先相手ユーザの変換された暗号アルゴリズムによるデスクランブル機能の確認

鍵管理用ワークステーションより送付された暗号文を、変換された暗号アルゴ

リズムのデスクランブル機能により復号しデスクランブル機能が正常に動作することを確認する。

【0206】

1: マスター鍵として P_{YIDC} を用いて、暗号文 $E_{ANG_{PYIDC}}(P_{TB})$ を復号し、セッション鍵 P_{TB} を取得する。

【0207】

2: セッション鍵 P_{TB} を用いて暗号文 $E_{ANG_{PTB}}(k_{DC})$ を復号し、デスクランブル鍵 k_{DC} を取得する。

【0208】

3: デスクランブル鍵 k_{DC} を用いて暗号文 $E_{k_{sc}}(MD)$ を復号し、平文データ MD を取得する。

【0209】

4: 平文データ MD が <アルゴリズム変換後のデスクランブル機能確認終了>であることを確認し、デスクランブル機能が正常動作することを確認する。

【0210】

(8) 送信先相手ユーザの変換された暗号アルゴリズムによるスクランブル機能の駆動

変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認するため、平文データを設定し、スクランブル機能で暗号化し鍵管理用ワークステーションに送付する。

【0211】

1: 平文データ MS を <アルゴリズム変換確認試験終了>とする。変換後の暗号アルゴリズム E_{ANG} でこの平文データ MS を暗号化するためのスクランブル鍵 K_{su} 、復号化するためのデスクランブル鍵 K_{du} を生成する。次に、データ MS をスクランブル鍵 k_{su} で暗号化し、暗号文 $E_{ANG_{ksu}}(MS)$ を作成し、同様にデスクランブル鍵 K_{du} を取得したセッション鍵 P_{TB} で暗号化し、暗号文 $E_{ANG_{PTB}}(k_{Du})$ を作成する。

【0212】

2: 作成した2組の暗号文 $E_{ANG_{PTB}}(k_{Du})$ 及び $E_{ANG_{ksu}}(MS)$ と

、鍵管理用ワークステーションから送付された暗号文 $E_{ANG_{PCIDC}}(P_{TB})$ とを鍵管理用ワークステーションに＜暗号アルゴリズム変換確認要求＞として返送する。

【0213】

(9) 鍵管理用ワークステーションでの暗号アルゴリズム変換の確認

送信先相手ユーザから返送された暗号文を復号し、送信先相手ユーザの変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【0214】

1: 鍵管理用ワークステーションのマスター鍵 P_{CIDC} を用いて、暗号文 $E_{ANG_{PCIDC}}(P_{TB})$ を復号し、セッション鍵 P_{TB} を取得する。

【0215】

2: セッション鍵 P_{TB} を用いて暗号文 $E_{ANG_{PTB}}(K_{DU})$ を復号し、デスクランブル鍵 K_{DU} を取得する。

【0216】

3: デスクランブル鍵 k_{Du} を用いて暗号文 $E_{ksu}(MS)$ を復号し、平文データ MS を取得する。

【0217】

4: 取得した平文データ MS が＜アルゴリズム変換確認試験終了＞であることを確認し、送信先相手ユーザのスクランブル機能が正常動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【0218】

このようにして、共通鍵暗号が運用されるネットワーク通信システムにおいて、アルゴリズム変換を実施することができる。

【0219】

このアルゴリズム変換により、ユーザ $U[A]$ とユーザ $U[B]$ とは、同一の暗号アルゴリズムを共有することになった。これにより、図7に示す手順により、ユーザ $U[A]$ とユーザ $U[B]$ とは暗号化通信を実施することが可能となった。

【0220】

本実施の形態において、ユーザU〔A〕とユーザU〔B〕とが、同一系列の暗号強度が同じか、または異なる暗号アルゴリズムを所有している場合は、ネットワーク暗号アルゴリズム管理機能により強度の強い暗号アルゴリズムに変換することも可能である。

【0221】

この場合、ユーザU〔A〕のほうがユーザU〔B〕より強い強度の暗号アルゴリズムをもっている場合は、ユーザU〔B〕をユーザU〔A〕の暗号アルゴリズムに変換することになり、逆に、ユーザU〔B〕のほうが強ければ、ユーザU〔A〕をユーザU〔B〕の暗号アルゴリズムに変換することになる。

【0222】

このアルゴリズム変換は、図6及び図8、9に示す手順と同様にして実行することができる。

【0223】

次に、鍵管理用ワークステーションが管理している暗号アルゴリズムの暗号強度を上げるか、または、暗号強度は変えずに暗号アルゴリズムのバージョンを変えてセキュリティを改善する例について示す。

【0224】

図1で示したように、暗号アルゴリズムA〔1〕～A〔n〕は、同一のA暗号系列の鍵管理用ワークステーションが管理している暗号アルゴリズムであり、鍵管理用ワークステーションはこの暗号のアルゴリズムを生成する機能を有している。暗号アルゴリズムを変更することにより、暗号強度を変えたり、暗号化演算の手順を変えることができ、同一の暗号アルゴリズムを使用することと比較すると、暗号化通信システムのセキュリティを改善することができる。

【0225】

同一のA系列の暗号アルゴリズムを運用するユーザのユーザIDは、U〔A_i, j〕であり、鍵管理用ワークステーションは、このユーザのなかから暗号アルゴリズムを変更するユーザを定める。そして、暗号のアルゴリズムを生成する機能を用いて、新しく暗号アルゴリズムを生成し、暗号アルゴリズムを変更すると

定めたユーザに新しく生成した暗号アルゴリズムを配信する。

【0226】

この配信は、前述した暗号アルゴリズムのアルゴリズム変換と同様に行うことができる。

【0227】

以上で、バージョンが異なる暗号アルゴリズム、暗号強度が異なる暗号アルゴリズムを配信する例について説明した。

【0228】

各ユーザに配信された暗号アルゴリズムに各ユーザの暗号アルゴリズムは変換されるわけであるが、変換前の暗号アルゴリズムは、消さないで各ユーザの暗号アルゴリズムDBに格納するようにし、鍵管理用ワークステーションは、各ユーザが暗号アルゴリズムDBに格納されている暗号アルゴリズムを、ネットワーク暗号アルゴリズム管理DBに管理するようにしておく。

【0229】

このようにしておくと、ユーザU〔A〕からユーザU〔B〕に暗号化通信要求が生じた場合、双方のユーザの暗号アルゴリズムDBに共通の暗号アルゴリズムが存在する場合は、鍵管理用ワークステーションが暗号アルゴリズムを配信する必要はなく、鍵管理用ワークステーションがこの共通の暗号アルゴリズムへ切り替えの指示を出せば、ユーザU〔A〕からユーザU〔B〕に暗号化通信が可能となる。

【0230】

以上、暗号化通信システムが共通鍵暗号で構成されている場合の暗号アルゴリズム変換のについて説明した。

【0231】

次に、図11から図15を参照して、本発明の第3の実施の形態について説明する。ここでは、公開鍵暗号が運用されるネットワーク通信システム、すなわち、暗号化通信システムが公開鍵暗号で構成されている場合の暗号アルゴリズム変換について説明する。

【0232】

図1に示すネットワーク通信システムにおいて、運用される暗号アルゴリズム $A[1] \sim A[n]$ 及び $B[1] \sim B[m]$ は、すべて公開鍵暗号アルゴリズムとする。

【0233】

図12を参照して、公開鍵暗号アルゴリズムによる暗号化通信について説明する。

【0234】

公開鍵暗号アルゴリズムとしては、例えば、楕円曲線暗号の暗号アルゴリズムを適用することができる。この楕円曲線暗号の鍵の演算を記載するのに必要な楕円曲線のベースポイントを P とする。楕円曲線暗号については、例えば、信学技報 TECHNICAL REPORT OF IEICE ISEC 97-15(1997-07)「楕円曲線を利用した高速暗号化法」宝木和夫、車谷博之に記載されている。

【0235】

暗号化通信を実施する場合、鍵管理用ワークステーションのネットワーク鍵管理機能からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のパーソナルコンピュータのデスクランブル機能に送信する。

【0236】

デスクランブル機能は、送付された暗号文を復号化し、データを取得する。

【0237】

暗号化通信処理部を運用する前提条件として、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理用ワークステーションより、ユーザ ID とマスター鍵として、秘密鍵 d_{ID} と、この秘密鍵に対応する公開鍵 Q_{ID} ($= P \cdot d_{ID}$; \cdot は楕円曲線上の演算) とを割り当てられており、鍵管理用ワークステーションのネットワーク鍵管理 DB に、ユーザに割り当てた公開鍵 Q_{ID} をユーザ ID と対応させて登録し管理している。同様に、鍵管理用ワークステーション自身にも、マスター鍵として、秘密鍵 d_C と、この秘密鍵に対応する公開鍵 Q_C ($= P \cdot d_C$; \cdot は楕円曲線上の演算) が割り当てられているものとし、鍵管理

用ワークステーション自身の公開鍵 Q_C は、本システムを利用するすべてのユーザに公開するものとする。

【0238】

本実施例では、データの暗号化をスクランブル鍵 K_S で行い、データの復号化をデスクランブル鍵 K_D で行うものとし、このデスクランブル鍵 K_D の配送を公開鍵暗号である楕円曲線暗号で実施するものとする。スクランブル鍵 K_S 、デスクランブル鍵 K_D を運用する共通鍵暗号アルゴリズムとしては、例えば、MULTI2暗号アルゴリズムを用いることができる。MULTI2暗号アルゴリズムは、CSデジタル放送などで実績がある暗号アルゴリズムである。

【0239】

以下、ユーザ $U[A]$ からユーザ $U[B]$ に暗号化通信を行う場合を例にとって説明する。ここで、ユーザ $U[A]$ は送信側ユーザとし、ユーザ $U[B]$ は受信側ユーザとする。

【0240】

(1) ユーザ $U[A]$ からユーザ $U[B]$ に暗号化通信を行う場合、ユーザ $U[A]$ は鍵管理用ワークステーションに、セッション鍵発行要求を行う。このセッション鍵発行要求を受けて、鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能は、ネットワーク暗号アルゴリズムDBの検索を行い、ユーザ $U[A]$ が使用している暗号アルゴリズムと、ユーザ $U[B]$ が使用している暗号アルゴリズムとが同一かどうかの判断を行う。

【0241】

(2) ユーザ $U[A]$ とユーザ $U[B]$ とが同一の暗号アルゴリズムを使用していると判断したとき、鍵管理用ワークステーションのネットワーク鍵管理機能は、ユーザIDをキーとしてネットワーク鍵管理DBを検索し、送信先相手ユーザのマスター鍵に対応する公開鍵 Q_{YID} と、送信側ユーザのマスター鍵に対応する公開鍵 Q_{ID} とを取り出す。

【0242】

取り出した公開鍵 Q_{YID} と公開鍵 Q_{ID} とに対して、鍵管理用ワークステーションのマスター鍵である秘密鍵 d_C で署名作成演算を実施し署名データ $S_{dc}(Q_{YID}$

)と署名データ $S_{dc}(Q_{ID})$ とを作成する。この公開鍵 Q_{YID} をセッション鍵とし署名データ $S_{dc}(Q_{YID})$ 及び署名データ $S_{dc}(Q_{ID})$ とを組み合わせて、送信側ユーザに送付しセッション鍵の発行を実施する。

【0243】

(3) 公開鍵 Q_{YID} と署名データ $S_{dc}(Q_{YID})$ 及び署名データ $S_{dc}(Q_{ID})$ を受信したユーザは、鍵管理用ワークステーションの公開鍵 Q_C を用いて署名データ $S_{dc}(Q_{YID})$ と Q_{YID} とに対し署名検証演算を実施し、公開鍵 Q_{YID} が正当な鍵管理用ワークステーションから送付されたものであることを確認し、通信しようとする正当な送信先相手ユーザに割り当てられた公開鍵であることを確認する。

【0244】

このようにして、送信側ユーザはセッション鍵として使用する公開鍵の発行を受ける。

【0245】

(4) 送信側のユーザは、送信するデータ M を暗号化するためのスクランブル鍵 K_S と復号するためのデスクランブル鍵 K_D を生成する。

【0246】

次にユーザの入力するデータ M をスクランブル鍵 K_S で暗号化し、暗号文 $E_{K_S}(M)$ を作成する。

【0247】

また、送付されたセッション鍵としての公開鍵 Q_{YID} でデスクランブル鍵 K_D を暗号化し、暗号化デスクランブル鍵 $E_{Q_{YID}}(K_D)$ を生成する。

【0248】

また、送信するデータ M が確実に送信側ユーザが作成したものであることを保証するため、鍵管理用ワークステーションより送信側ユーザに割り当てられているマスター鍵としての秘密鍵 d_{ID} で、送信するデータ M に署名作成演算を実施し、署名データ $S_{dID}(M)$ を作成する。

【0249】

公開鍵暗号の場合、送付された鍵 Q_{YID} は、そのまま暗号化のための鍵として

使用することができる。

【0250】

このようにして作成した2組の暗号文 $E_{K_S}(M)$ 及び $E_{Q_{YID}}(K_D)$ と、データMに関する署名データ $S_{dID}(M)$ と、鍵管理用ワークステーションより送付された送信側ユーザの公開鍵に関する署名データ $S_{dc}(Q_{ID})$ 及び送信側ユーザ自身の公開鍵 Q_{ID} との5組のデータを送信相手先のユーザに送信する。

【0251】

(5) 5組のデータを受信した送信相手先のユーザは、まず鍵管理用ワークステーションの公開鍵 Q_c を用いて署名データ $S_{dc}(Q_{ID})$ 及び Q_{ID} に対し署名検証演算を実施し、公開鍵 Q_{ID} が正当な鍵管理用ワークステーションから送付されたものであることを確認し、正当な送信側ユーザに割り当てられた公開鍵であることを確認する。

【0252】

鍵管理用ワークステーションより送信相手先のユーザに割り当てられているマスター鍵としての秘密鍵 d_{YID} で、暗号化デスクランブル鍵 $E_{Q_{YID}}(K_D)$ を復号し、デスクランブル鍵 K_D を取得する。

【0253】

次に、このデスクランブル鍵 K_D を用いて、暗号文 $E_{K_S}(M)$ を復号し、データMを得る。

【0254】

最後に、送信側ユーザから送付された公開鍵 Q_{ID} を用いて署名データ $S_{dID}(M)$ とデータMとに対し署名検証演算を実施し、データMが正当な送信側ユーザから伝達されたデータであることを確認する。

【0255】

このようにして、ネットワーク通信システムにおいて、ユーザU[A]からユーザU[B]に対して暗号化通信を行うことが可能となる。

【0256】

一方、暗号アルゴリズム管理機能がユーザU[A]とユーザU[B]とが同一の暗号アルゴリズムを使用していないと判断すると、ユーザU[B]の暗号アル

ゴリズムの変換を実施し、ユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを運用できるようにする。

【0257】

以下、図11及び図13、14を参照して、公開鍵暗号アルゴリズムが運用されるネットワーク通信システムにおける暗号アルゴリズム変換について説明する。

【0258】

(1) ネットワーク暗号アルゴリズム管理機能は、送信側のユーザから、送信側ユーザのユーザIDと送信先相手ユーザのユーザIDとを付加したセッション鍵発行要求を受けると、送付されたユーザIDをキーとしてネットワーク暗号アルゴリズム管理DBの検索を実施し、送信側ユーザと送信先相手ユーザが運用する暗号アルゴリズムの状態を把握する。図11に示すようにネットワーク通信システムは、二重暗号方式の暗号化通信システムをとっており、データの暗号化に共通鍵暗号アルゴリズムを用い、セッション鍵の運用に公開鍵の暗号アルゴリズムを用いている。

【0259】

送信側ユーザと送信先相手ユーザとが運用する二種類の暗号アルゴリズムが一致しないと、両者の間で暗号化通信を実施することはできない。

【0260】

ネットワーク暗号アルゴリズム管理DBを検索の結果、一致しない場合、送信側ユーザの運用する暗号アルゴリズムEANGを取り出す。取り出した暗号アルゴリズムには、データの暗号化に用いるものか、セッション鍵の運用に用いるかの識別子を付加するものとする。当然、二種類の暗号アルゴリズムが両方一致しなければ、二種類の暗号アルゴリズムを取り出すことになる。

【0261】

送信先相手ユーザの運用している暗号アルゴリズムをEBFとすると、この暗号アルゴリズムEBFから取り出した暗号アルゴリズムEANGに暗号アルゴリズムを変換させることになる。

【0262】

(2) 鍵管理用ワークステーションのネットワーク鍵管理機能は、ユーザIDをキーとしてネットワーク鍵管理DBを検索し変換前の暗号アルゴリズムEBFの送信先相手ユーザのマスター鍵に対応する公開鍵 Q_{YID} を取り出す。

【0263】

暗号アルゴリズムEANGに変換された場合、送信先相手ユーザの変換前の暗号アルゴリズムEBFでのマスター鍵が使用できなくなる場合がある。この場合、ネットワーク鍵管理機能は暗号アルゴリズムの変換に対して送信先相手ユーザのマスター鍵に互換性があるか無いかの判断を行い、互換性が無いと判断した場合は、新規に送信先相手ユーザの公開鍵を生成する。

【0264】

新しく生成したマスター鍵としての秘密鍵を d_{YIDC} としこの秘密鍵に対応する公開鍵を Q_{YIDC} とする。

【0265】

鍵管理用ワークステーションは、変換前の暗号アルゴリズムEBF、及び、変換後の暗号アルゴリズムEANGのどちらの暗号アルゴリズムに対しても対応するマスター鍵が割り当てられている。

【0266】

変換前の暗号アルゴリズムEBFに対応するマスター鍵としての秘密鍵を d_C としこの秘密鍵に対応する公開鍵を Q_C とする。

【0267】

変換後の暗号アルゴリズムEANGに適応するマスター鍵としての秘密鍵を d_{CG} としこの秘密鍵に対応する公開鍵を Q_{CG} とする。

【0268】

(3) ネットワーク鍵管理機能は、変換前の暗号アルゴリズムEBFを使用して、以下の暗号文及び、署名データを作成する。

【0269】

1: 変換前の暗号アルゴリズムEBFで暗号アルゴリズムEANG及び秘密鍵 d_{YIDC} を暗号化するためのスクランブル鍵 K_{SB} 、復号化するためのデスクラン

ブル鍵 K_{DB} を生成する。

【0270】

2: 暗号アルゴリズムEANG及び秘密鍵 d_{YIDC} をスクランブル鍵 k_{SB} で暗号化し、暗号文 $E B F_{KSB}(EANG)$ と暗号文 $E B F_{KSB}(d_{YIDC})$ を作成する。また、取り出したマスター鍵としての公開鍵 Q_{YID} でデスクランブル鍵 K_{DB} を暗号化し、暗号文 $E B F_{QYID}(K_{DB})$ を作成する。

【0271】

3: 変換前の暗号アルゴリズムEBFと鍵管理用ワークステーションのマスター鍵である秘密鍵 d_c で、新しく生成した秘密鍵 d_{YIDC} と公開鍵 Q_{YIDC} に対し署名作成演算を実施し、署名データ $S_{dc}(d_{YIDC})$ 及び署名データ $S_{dc}(Q_{YIDC})$ を作成する。

【0272】

4: 変換前の暗号アルゴリズムEBFと鍵管理用ワークステーションのマスター鍵である秘密鍵 d_c で、暗号アルゴリズムEANGに対し署名作成演算を実施し、署名データ $S_{dc}(EANG)$ を作成する。

【0273】

5: 変換前の暗号アルゴリズムEBFと鍵管理用ワークステーションのマスター鍵である秘密鍵 d_c で、変換後の暗号アルゴリズムEANGに適用する鍵管理用ワークステーションのマスター鍵としての公開鍵 Q_{CG} に対して署名作成演算を実施し、署名データ $S_{dc}(Q_{CG})$ を作成する。

【0274】

(4) スクランブル機能は、変換後の暗号アルゴリズムEANGを使用して、以下の暗号文及び、署名データを作成する。

【0275】

1: 平文データMDを<アルゴリズム変換後のデスクランブル機能確認終了>とする。

【0276】

変換後の暗号アルゴリズムEANGで、前記平文データMDを暗号化するためのスクランブル鍵 K_{SC} 、復号化するためのデスクランブル鍵 K_{DC} を生成する。次

にデータMDをスクランブル鍵 K_{sc} で暗号化し、暗号文 $EANG_{KSC}(MD)$ を作成し、同様にデスクランブル鍵 K_{DC} を変換後の暗号アルゴリズムで運用するセッション鍵として運用する公開鍵 Q_{YIDC} で暗号化し、暗号文 $EANG_{QYIDC}(K_D)$ を作成する。

【0277】

2: 変換後の暗号アルゴリズム $EANG$ で鍵管理用ワークステーションのマスター鍵とし割り当てられている秘密鍵 d_{cg} で、新しく生成した公開鍵 Q_{YIDC} と、平文データMDとに対して署名作成演算を実施し、署名データ $S_{dcg}(Q_{YIDC})$ 、 $S_{dcg}(MD)$ を作成する。

【0278】

(5) 前記(3)項で作成した3組の暗号文 $EBF_{QYID}(K_{DB})$ 、 $EBF_{KSB}(EANG)$ 及び $EBF_{KSB}(d_{YIDC})$ と、4組の署名データ $S_{dc}(d_{YIDC})$ 、 $S_{dc}(Q_{YIDC})$ 、 $S_{dc}(EANG)$ 及び $S_{dc}(Q_{CG})$ と、新しく生成した公開鍵 Q_{YIDC} と、鍵管理用ワークステーションの公開鍵 Q_{CG} と、前記(4)項で作成した2組の暗号文 $EANG_{KSC}(MD)$ 及び $EANG_{QYIDC}(K_{DC})$ 並びに2組の署名データ $S_{dcg}(Q_{YIDC})$ 、 $S_{dcg}(MD)$ とを<暗号アルゴリズム変換要求>として送信先相手ユーザに送付する。ここで、前記(3)項で作成した暗号文及び署名データは、送信先相手ユーザの暗号アルゴリズムを変換するための情報であり、前記(4)項で作成した4組の暗号文及び署名データは、暗号アルゴリズムを変換後、変換した暗号アルゴリズムが正常に機能するか確認するための情報である。

【0279】

ネットワーク鍵管理機能は、新しく生成した送信先相手ユーザのマスター鍵としての公開鍵 Q_{YIDC} をネットワーク鍵管理DBに暗号アルゴリズム $EANG$ と対応させて格納する。

【0280】

(6) 送信先相手ユーザの暗号アルゴリズムの変換、及びマスター鍵の更新
送信先相手ユーザは、暗号アルゴリズムとして EBF を運用しており、マスター鍵としての秘密鍵 d_{YID} 、及び暗号アルゴリズム EBF で運用される鍵管理用

ワークステーションの公開鍵 Q_C を所有している。

【0281】

鍵管理用ワークステーションより送付された暗号文から、

1: マスター鍵として秘密鍵 d_{YID} を用いて、暗号文 $EBF_{QYID}(K_{DB})$ を復号し、デスクランブル鍵 K_{DB} を取得する。次にこのデスクランブル鍵 K_{DB} を用いて暗号文 $EBF_{KSB}(EANG)$ を復号し、暗号アルゴリズム $EANG$ を取得する。鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(EANG)$ と、取得した暗号アルゴリズム $EANG$ とに対して署名検証演算を実施し、取得した暗号アルゴリズム $EANG$ が正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【0282】

2: デスクランブル鍵 K_{DB} を用いて、暗号文 $EBF_{KSB}(d_{YIDC})$ を復号し、変換した暗号アルゴリズム $EANG$ 上で運用する、当該ユーザのマスター鍵として秘密鍵 d_{YIDC} を取得する。

【0283】

鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(d_{YIDC})$ と、取得した秘密鍵 d_{YIDC} とに対して署名検証演算を実施し、取得した取得した秘密鍵 d_{YIDC} が正当な鍵管理用ワークステーションから送付されたものであることを確認する。同様に、鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(Q_{YIDC})$ と、送付されたマスター鍵である公開鍵 Q_{YIDC} とに対して署名検証演算を実施し、取得した取得した公開鍵 Q_{YIDC} が正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【0284】

3: 鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(Q_{CG})$ と、送付された鍵管理用ワークステーションの変換した暗号アルゴリズム $EANG$ 上で運用する公開鍵 Q_{CG} とに対して署名検証演算を実施し、送付された公開鍵 Q_{CG} が正当な鍵管理用ワークステーションの公開鍵であることを確認する。

【0285】

以上のようにして、送信先相手ユーザは、暗号アルゴリズムEANGと、マスター鍵としての秘密鍵 d_{YIDC} と、この秘密鍵に対応する公開鍵 Q_{YIDC} と、鍵管理用ワークステーションの変換した暗号アルゴリズムEANG上で運用する公開鍵 Q_{CG} とを取得した。これらにより、取得した暗号アルゴリズムEANGを暗号アルゴリズム管理DBに登録するとともに、暗号アルゴリズム管理機能によって運用する暗号アルゴリズムを、暗号アルゴリズムEBFから暗号アルゴリズムEANGに変換する。

【0286】

送信先相手ユーザのマスター鍵が変更になる場合は、鍵構成管理機能によりマスター鍵としての秘密鍵を d_{YID} から d_{YIDC} に更新する。

【0287】

(7) 送信先相手ユーザの変換された暗号アルゴリズムによるデスクランブル機能の確認

鍵管理用ワークステーションより送付された暗号文を、変換された暗号アルゴリズムのデスクランブル機能により復号しデスクランブル機能が正常に動作することを確認する。

【0288】

1: マスター鍵として秘密鍵 d_{YIDC} を用いて、暗号文 $EANG_{Q_{YIDC}}$ (K_{DC})を復号し、デスクランブル鍵 K_{DC} を取得する。

【0289】

2: デスクランブル鍵 K_{DC} を用いて暗号文 $EANG_{K_{SC}}$ (MD)を復号し、平文データMDを取得する。次に、鍵管理用ワークステーションの公開鍵 Q_{CG} を用いて、署名データ S_{dcg} (MD)と取得した平文データMDとに対して署名検証演算を実施し、取得した平文データMDが正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【0290】

3: 平文データMDが<アルゴリズム変換後のデスクランブル機能確認終了>であることを確認し、デスクランブル機能が正常動作することを確認する。

【0291】

(8) 送信先相手ユーザの変換された暗号アルゴリズムによるスクランブル機能の駆動

変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認するため、平文データを設定し、スクランブル機能で暗号化し鍵管理用ワークステーションに送付する。

【0292】

1: 平文データMSを<アルゴリズム変換確認試験終了>とする。変換後の暗号アルゴリズムEANGで前記平文データMSを暗号化するためのスクランブル鍵 K_{SU} 及び復号化するためのデスクランブル鍵 K_{DU} を生成する。次に、平文データMSをスクランブル鍵 K_{SU} で暗号化し、暗号文 $EANG_{KSU}(MS)$ を作成し、同様に、デスクランブル鍵 K_{DU} を鍵管理用ワークステーションの公開鍵 Q_{CG} で暗号化し、暗号文 $EANG_{QCG}(K_{DU})$ を作成する。また、データMSに対して送信先相手ユーザのマスター鍵としての秘密鍵 d_{YIDC} を用いて署名作成演算を実施し、署名データ $S_{dYIDC}(MS)$ を作成する。

【0293】

2: 作成した2組の暗号文 $EANG_{QCG}(K_{DU})$ 及び $EANG_{KSU}(MS)$ と、署名データ $S_{dYIDC}(MS)$ と、鍵管理用ワークステーションから送付された署名データ $S_{dcg}(Q_{YIDC})$ と、送信先相手ユーザの公開鍵 Q_{YIDC} とを<暗号アルゴリズム変換確認要求>として鍵管理用ワークステーションに返送する。

【0294】

(9) 鍵管理用ワークステーションでの暗号アルゴリズム変換の確認

送信先相手ユーザから返送された暗号文を復号し、送信先相手ユーザの変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【0295】

1: 鍵管理用ワークステーションのマスター鍵としての秘密鍵 d_{cg} を用いて、暗号文 $EANG_{QCG}(K_{DU})$ を復号し、デスクランブル鍵 K_{DU} を取得する。

【0296】

2: デスクランブル鍵 K_{DU} を用いて暗号文 $EANG_{ksu}$ (MS)を復号し、平文データMSを取得する。

【0297】

3: 鍵管理用ワークステーションの公開鍵 Q_{cg} を用いて、署名データ S_{dcg} (Q_{YIDC})と送付された送信先相手ユーザの公開鍵 Q_{YIDC} に対して署名検証演算を実施し、付された送信先相手ユーザの公開鍵 Q_{YIDC} が正当な送信先相手ユーザ、すなわち受信側ユーザから送付されたものであることを確認する。

【0298】

4: 送信先相手ユーザの公開鍵 Q_{YIDC} を用いて、署名データ S_{dYIDC} (MS)と取得した平文データMSに対して署名検証演算を実施し、取得した平文データMSが正当な送信先相手ユーザ、すなわち受信側ユーザから送付されたものであることを確認する。

【0299】

5: 取得した平文データMSが<アルゴリズム変換確認試験終了>であることを確認し、送信先相手ユーザのスクランブル機能が正常動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【0300】

以上の(1)～(9)により、本実施の形態におけるアルゴリズム変換の実施例について示した。この暗号アルゴリズム変換により、ユーザU[A]とユーザU[B]とは、同一の暗号アルゴリズムを共有することになった。これにより、図12に示されるようにして、ユーザU[A]とユーザU[B]との間で暗号化通信を実施することが可能となった。

【0301】

暗号アルゴリズムを変換した場合、本実施例では、ユーザの所有するマスター鍵としての秘密鍵と、この秘密鍵に対応する公開鍵とを、鍵管理用ワークステーションで新しく生成している。

【0302】

これらの鍵は、全く新しく生成してもよいが、変換前の鍵をもとに生成するこ

とも可能である。以下、この鍵の生成について説明する。

【0303】

公開鍵暗号の場合も暗号化通信に使用する秘密鍵は、共通鍵暗号の場合と同様、暗号アルゴリズム変換により、秘密鍵の鍵長すなわちビット数は、長くなったり、短くなったりする。

【0304】

鍵のビット数が短くなる場合は、送信先相手ユーザの変換前のマスター鍵としての秘密鍵 d_{YID} の後ろの冗長分のビット数を削除し、これを新しく送信先相手ユーザのマスター鍵としての秘密鍵 d_{YIDC} とする。

【0305】

鍵のビット数が長くなる場合は、図 15 に示すように、不足分のビット数に合わせて乱数 YR を生成し、 d_{PYID} に YR をつないで、新しく送信先相手ユーザのマスター鍵としての秘密鍵 d_{YIDC} ($d_{YIDC} = P_{YID} \parallel YR$) とする。

【0306】

生成した秘密鍵 d_{YIDC} に対応して公開鍵 Q_{YIDC} ($= P \cdot d_{YIDC}$; \cdot は楕円曲線上の演算) が定まる。

【0307】

この公開鍵 Q_{YIDC} が、以前に生成した他のユーザの秘密鍵になっている可能性もあるため、鍵管理用ワークステーションは、ネットワーク暗号アルゴリズム管理 DB を検索し、同じ公開鍵がないことを確認する。もし同じ公開鍵が存在するようならば、再度乱数を生成しマスター鍵としての秘密鍵を生成する。

【0308】

ここで、 YR として、常に 0 の値を使用することも可能である。

【0309】

マスター鍵、セッション鍵を運用する暗号アルゴリズムは、前述のように共通鍵暗号アルゴリズムとは異なる楕円曲線暗号アルゴリズムを用いており、これにより、二重暗号方式が構成され、セキュリティの向上が図られている。

【0310】

次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲

線暗号を用いた場合の鍵管理部について説明する。公開鍵暗号を用いた場合の鍵管理部のソフト機能は、図2に示す共通鍵暗号の場合のソフト機能と同じである。前述の公開鍵暗号アルゴリズムを使用した場合の暗号化処理部、及びアクセス管理部のソフト機能構成の実施例に示すように、各ユーザのマスター鍵は秘密鍵 d_{ID} であり、この秘密鍵と楕円曲線上の演算で公開鍵 $Q_{ID} (= d_{ID} \cdot P ; \cdot$ は楕円曲線上の演算) が対応している。また、スクランブル鍵及びデスクランブル鍵の暗号アルゴリズムは、共通鍵暗号アルゴリズムとしてMULTI2暗号アルゴリズムとしている。

【0311】

次に、本発明の第4の実施の形態について説明する。ここでは、可搬型の情報処理装置に組み込まれている暗号機能における暗号アルゴリズムの変換について説明する。

【0312】

上述の第1から第3の実施の形態においては、図1に示すように複数の暗号アルゴリズムがネットワーク通信システムに存在し、鍵管理用ワークステーションが各ユーザの暗号アルゴリズムの状態を把握し、暗号化通信の要求が発生するごとに、必要に応じてこの鍵管理用ワークステーションが各ユーザの暗号アルゴリズムを変換し、ユーザ間の暗号化通信を実施するようにしている場合について説明した。

【0313】

上述の説明では、図1に示すように複数の暗号アルゴリズムがネットワーク通信システムに存在し、鍵管理局用ワークステーションが各ユーザの暗号アルゴリズムの状態を把握し、暗号化通信の要求が発生するごとに、必要に応じてこの鍵管理局用ワークステーションが各ユーザの暗号アルゴリズムを変換し、ユーザ間の暗号化通信を実施するようにしている。

【0314】

ところが、近年、可搬型の情報処理装置、例えば、携帯端末装置、ICカードなどに、暗号機能が組み込まれ、電子マネーなどの自動支払いなどに使用されるようになった。

【0315】

すなわち、ユーザは、暗号機能が組み込まれた情報処理装置としてのICカードを所有し、電子マネーなどを自動支払いする場合、このICカードを店舗等に設置された情報処理装置としての読取り機にさし込み、両者の情報処理によって、支払いなどの決済を行う。

【0316】

この場合、ICカードが鍵管理局用ワークステーションと接続して、暗号処理を実施するのは、ユーザの手続きが煩雑となり、不便である。

【0317】

以下、可搬型の情報処理装置（端末、ICカードなど）で運用される暗号アルゴリズム変換に好適な暗号アルゴリズム変換方式について説明する。

【0318】

図12に示す、公開鍵暗号アルゴリズムで運用される暗号化通信システムにおいて、暗号化通信を実施する際、図2で示したように、送信側ユーザは、鍵管理用ワークステーションに〈セッション鍵発行要求〉を行い、該鍵管理用ワークステーションから、送信先相手ユーザの公開鍵 Q_{YID} 及び該公開鍵 Q_{YID} の署名データ $S_{dc}(Q_{YID})$ と、自分自身の公開鍵 Q_{ID} 及び該公開鍵 Q_{ID} の署名データ $S_{dc}(Q_{ID})$ との発行を受ける。

【0319】

ここで、各自の公開鍵 Q_{ID} 及び署名データ $S_{dc}(Q_{ID})$ とを各ユーザが鍵構成管理DBに格納するようにしておく。すなわち、公開鍵暗号アルゴリズムで運用される暗号化通信システムを図16に示す方式（該方式を機能ブロック図で表すと図25のようになる）とし、各ユーザが自分自身の公開鍵 Q_{ID} 及び該公開鍵 Q_{ID} の署名データ $S_{dc}(Q_{ID})$ を、予め鍵管理用ワークステーションから、図16における点線で示すルートで配布されて受け取り、各ユーザの鍵構成管理DBに所有するようにしておけば、暗号化通信を実施する際の〈セッション鍵発行要求〉を鍵管理用ワークステーションにするのではなく、送信先相手ユーザにすることが出来る。

【0320】

すなわち、＜セッション鍵発行要求＞を送信先相手ユーザに送付し、送信先相手ユーザから相手ユーザの公開鍵 Q_{YID} と、この公開鍵の署名データ $S_{dc}(Q_{YID})$ との送付を受ける。

【0321】

図16に示す方式において、各ユーザに割り当てるマスター鍵としての秘密鍵 d_{ID} は、鍵管理用ワークステーションが生成する方式と、各ユーザが生成する方式とが考えられる。

【0322】

1： 鍵管理用ワークステーションが生成する方式

マスター鍵としての秘密鍵 d_{ID} 及び対応する公開鍵 Q_{ID} を鍵管理用ワークステーションが生成してくれれば、暗号アルゴリズムの運用に不慣れなユーザにとっては非常に便利である。

【0323】

しかし、各ユーザにどのようにして生成した秘密鍵を配布するかが問題となる。

【0324】

本実施の形態では、ICカードやフロッピーディスクなどの電子媒体に格納し、ユーザに確実に配布することにする。

【0325】

生成した秘密鍵 d_{ID} を鍵管理用ワークステーションが保持することになると、ユーザが対応する公開鍵 Q_{ID} で暗号化するデータを鍵管理用ワークステーションがすべて解読することが可能となる。このように、鍵管理用ワークステーションが、ユーザの情報を握ることを防止するため、本実施の形態では、生成した秘密鍵 d_{ID} に鍵回復機能を持たせ、ネットワーク鍵構成DBに、ユーザIDと対応させて保存するようにし、不測の事態以外は、ユーザが作成した暗号文を解読できないようにする。

【0326】

以下に、本実施の形態における鍵回復機能について、鍵が二重の階層構造を有

する暗号化通信を例にとって説明する。鍵回復機能は、暗号文 $E_{KS}(M)$ に解読の情報を付加し、デスクランブル鍵 K_D によらずに暗号文を解読する手段を与えるものである。

【0327】

まず、次に、共通鍵暗号アルゴリズムによる暗号化通信における鍵回復機能について説明する。すなわち、ユーザが送信するデータを M とし、可搬型の情報処理装置が生成するスクランブル鍵 K_S によりデータは暗号化され、暗号文 $E_{KS}(M)$ が作成される。この暗号文を復号するためのデスクランブル鍵 K_D を、鍵管理用ワークステーションから送付されたセッション鍵 P_T によって暗号化し、暗号文 $E_{PT}(K_D)$ を作成している。

【0328】

まず、図23を参照して、スクランブル鍵 K_S でデータを暗号化する際、鍵回復機能を持たせるための付加データの作成手順について説明する。

【0329】

(1) スクリンブル鍵 K_S を生成するとき、乱数を生成し K_1 , K_2 の排他的論理和 (XOR、図では、直和記号で示している。) により、スクランブル鍵を $K_S = K_1 \text{ XOR } K_2$ と表現できるようにする。

【0330】

(2) P_1 , P_2 を鍵回復用の鍵とし、可搬型の情報処理装置及び、鍵管理用ワークステーションの鍵回復機能で保管するものとする。スクランブル鍵 K_S を生成するときに生成した K_1 , K_2 をこの鍵回復用の鍵 P_1 , P_2 で暗号化して暗号文 $E_{P1}(K_1)$, $E_{P2}(K_2)$ を作成する。このデータを、スクランブル鍵 K_S で作成したデータの暗号文 $E_{KS}(M)$ に付加するものとする。

【0331】

次に、図24を参照して、この付加データで暗号文を復号する手順について説明する。

【0332】

(1) 暗号文から付加されたデータ $E_{P1}(K_1)$, $E_{P2}(K_2)$ を分離し、鍵回復用の鍵 P_1 , P_2 で K_1 , K_2 を復号する。

【0333】

(2) K_1 , K_2 の排他的論理和を取り、 $K_S = K_1 \text{ XOR } K_2$ として、スクランブル鍵 K_S を生成する。共通鍵暗号の場合、スクランブル鍵 K_S とデスクランブル鍵 K_D とは同一であり、このスクランブル鍵 K_S により、暗号文を復号することができる。

【0334】

不測の事態が発生して、暗号文を解読する必要が生じた場合、暗号文を鍵管理用ワークステーションに送付すれば、前記に示した手順により、鍵回復用の鍵 P_1 , P_2 を用いて暗号文を解読することができる。

【0335】

次に、公開鍵暗号アルゴリズムによる暗号化通信における鍵回復機能について説明する。すなわち、データ M の暗号化に用いるスクランブル鍵を K_S , デスクランブル鍵を K_D とし、デスクランブル鍵を配送するためのセッション鍵としての公開鍵を Q_{YID} とすると、暗号化通信は、暗号文 $E_{KS}(M)$ と暗号化デスクランブル鍵 $E_{QYID}(K_D)$ の送信により実施される。

【0336】

ここでは、公開鍵暗号として楕円曲線暗号を用いられる場合を例にとって説明する。楕円曲線暗号については、例えば、信学技報 TECHNICAL REPORT OF IEICE ISEC97-15 (1997-07) の「楕円曲線を利用した高速暗号化方法」 宝木和夫, 車谷博之に記載されている。

【0337】

まず、暗号化デスクランブル鍵 $E_{QYID}(K_D)$ にしきい値ロジックを付加する鍵回復機能について説明する。

【0338】

(1) 鍵管理用ワークステーションの鍵回復機能において、鍵回復用の公開鍵 Q_A , Q_B , Q_C を割り当て、公開するとともに、この公開鍵に対応する秘密鍵 d_A , d_B , d_C ($Q_A = d_A \cdot P$, $Q_B = d_B \cdot P$, $Q_C = d_C \cdot P$) を保管するものとする。

【0339】

暗号化デスクランブル鍵 $E_{QYID}(K_D)$ には、鍵 Q_{YID} 、 Q_A 、 Q_B 、 Q_C で算出されるしきい値ロジックを付加するものとする。

【0340】

(2) 共通鍵暗号を用いた場合と同様、暗号化通信を行う場合、デスクランブル鍵 K_D を暗号化してからでないと、データをスクランブル鍵 K_S で暗号化できないようにし、データの暗号文 $E_{KS}(M)$ と暗号化デスクランブル鍵 $E_{QYID}(K_D)$ は必ずペアで生成されるようにする。

【0341】

(3) 不測の事態が発生して暗号文を解読する必要が生じた場合、ペアとなった暗号文 $E_{KS}(M)$ 、 $E_{QYID}(K_D)$ を鍵管理ワークステーションに送付する。

【0342】

鍵回復機能では、秘密鍵 d_A 、 d_B 、 d_C の2つと、 $E_{QYID}(K_D)$ に付加されたしきい値ロジックを用いて復号し、デスクランブル鍵 K_D を取得する。

【0343】

次に、この鍵 K_D で暗号文 $E_{KS}(M)$ を復号し、データ M を取得する。

【0344】

ここで、送信するデータ M の暗号文は、スクランブル鍵 K_S による暗号化演算で作成される。このため、共通鍵暗号を用いた鍵回復機能（暗号化について図23、復号化について図24参照）と全く同様に、スクランブル鍵 K_S を K_1 、 K_2 の排他的論理和で表現し、これを用いて鍵回復を実施する方法をとることもできる。図23、図24に示す鍵回復用の鍵 P_1 、 P_2 は、共通鍵暗号アルゴリズムで運用することもできるが、鍵回復用として、公開鍵 Q_A 、 Q_B により運用することも可能である。

【0345】

この場合暗号文 $E_{KS}(M)$ に鍵回復用として付加するデータは、 K_1 、 K_2 を公開鍵 Q_A 、 Q_B により暗号化した暗号文 $E_{QA}(K_1)$ 、 $E_{QB}(K_2)$ であり、鍵回復は、鍵管理用ワークステーションの鍵回復機能において公開鍵 Q_A 、 Q_B に対応する秘密鍵 d_A 、 d_B を用いて、付加されたデータを復号することにより実施す

る。

【0346】

2： 各ユーザが生成する方式

暗号アルゴリズムの運用に慣れているユーザは、自分自身が使用するマスター鍵としての秘密鍵 d_{ID} 及び対応する公開鍵 Q_{ID} を自ら生成することも可能である。

【0347】

この場合、ユーザが所有するマスター鍵としての秘密鍵 d_{ID} は、当該ユーザのみが所有するため、公開鍵 Q_{ID} で作成した暗号文を鍵管理用ワークステーションから解読される可能性は、まったくない。

【0348】

当該ユーザは、秘密鍵 d_{ID} に対応して生成した公開鍵 Q_{ID} を鍵管理用ワークステーションに送付する。

【0349】

鍵管理用ワークステーションは、公開鍵 Q_{ID} を送付した当該ユーザの身元を確認し、送付された公開鍵 Q_{ID} に、鍵管理用ワークステーションの所有する秘密鍵 d_c により署名作成演算を実施し、署名データ $S_{dc}(Q_{ID})$ を当該ユーザに送付する。

【0350】

本実施の形態では、1：項で示した場合と同様、ユーザの所有するマスター鍵としての秘密鍵 d_{ID} は、鍵回復機能を持たせ、ネットワーク鍵構成DBに、ユーザIDと対応させて保存するようにする。

【0351】

各ユーザが所有するマスター鍵としての秘密鍵 d_{ID} 及び、対応する公開鍵 Q_{ID} を鍵管理用ワークステーションが生成するか、ユーザが生成するかは、ユーザの事情に応じて、ユーザが選択するものとする。

【0352】

以上のような方式をとることにより、ICカードと店舗等に設置された情報処理装置としての読取り機とは、鍵管理用ワークステーションを経由せず、ICカ

ードを店舗等に設置された情報処理装置としての読取り機に挿し込んだ状態で暗号化通信を実施することができる。

【0353】

ユーザがICカードを情報処理装置としての読取り機に挿し込んだ時、ICカードと報処理装置としての読取り機の暗号アルゴリズムが異なる場合、両者の暗号アルゴリズムを同一にしなければ、暗号化通信、すなわち支払いなどの決済を実施することができない。

【0354】

この場合、暗号アルゴリズム変換を実施する必要があるが、ICカードを店舗等に設置された情報処理装置としての読取り機にさし込んだままこの暗号アルゴリズム変換が実施できれば、ユーザの手続きは簡便となり便利である。

【0355】

図17、図18を参照して、このような暗号アルゴリズム変換について説明する。

【0356】

暗号としては、前述の楕円曲線暗号とする。楕円曲線暗号の場合、楕円曲線 $Y^2 = X^3 + ax + b$ の係数 a 及び b と、係数の標数 p と、ベースポイント P 及びその位数 n とで暗号アルゴリズムが定まり、この暗号アルゴリズムは、秘匿してもよいし、また、公開してもよい。

【0357】

楕円曲線暗号の公開鍵 Q と秘密鍵 d とは、ベースポイント P により、 $Q = d \cdot P$ （ \cdot は、楕円曲線上の演算）と表される。

【0358】

楕円曲線 $y^2 = x^3 + ax + b$ の係数 a 、 b が同じでも、ベースポイント P を変更することにより、同じ暗号強度の別の暗号アルゴリズムを与えることができる。係数 a 、 b および係数の標数 p を変更すると、楕円曲線が変わり、別の暗号アルゴリズムが定まる。

【0359】

係数 a 、 b および係数の標数 p の変更の前後で、同程度の鍵長となるように、

楕円曲線を生成すれば、同程度の、暗号強度の相異なる複数の暗号アルゴリズムを与えることができる。

【0360】

係数 a 、 b および係数の標数 p を変更する場合、楕円曲線の生成法によっては、暗号強度、すなわち鍵長を変更することも可能である。

【0361】

以下、ICカードが使用している暗号アルゴリズムを EBF、情報処理装置としての読取り機の使用している暗号アルゴリズムを EANG とし、EBF の鍵長よりも EANG の鍵長のほうが長いと仮定した場合を例にとって、暗号アルゴリズム変換の実施態様について説明する。

【0362】

ここで、図 21 を参照して、暗号アルゴリズム変換の対象とする暗号化通信システムについて説明する。この暗号化通信システムは、暗号鍵が一重の階層構造をとっている。すなわち、図 16 示される暗号化通信システムでのスクランブル鍵と、デスクランブル鍵とを運用せずに暗号化通信システムが構築している。

【0363】

まず、図 3 のネットワーク通信システムのソフト機能を参照し、送信側ユーザ、受信側ユーザ、及びネットワーク管理用ワークステーションがそれぞれ所有している、鍵と暗号アルゴリズムに関する DB について説明する。本実施の形態では、送信側ユーザが情報処理装置としての読取り機に対応し、また、受信側ユーザが IC カードなどの可搬型の情報処理装置に対応している。

【0364】

図 19 を参照して、この鍵と暗号アルゴリズムに関する DB に格納される情報の具体例について説明する。

【0365】

(1) 鍵管理用ワークステーションの DB について

1: ネットワーク暗号アルゴリズム管理 DB

本ネットワーク通信システムで使用するすべての楕円曲線の暗号アルゴリズム $A[1]$ 、 $A[2]$ 、 \dots 、 $A[N]$ と、各暗号アルゴリズムに対応するバージョン

ン番号 $V_B[1]$, $V_B[2]$, ..., $V_B[N]$ と、この暗号アルゴリズムに対し
て鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 $d_C[1]$
, $d_C[2]$, ..., $d_C[N]$ と、この秘密鍵に対応する公開鍵 $Q_C[1]$, $Q_C[2]$, ..., $Q_C[N]$ とをおのの対応させて格納するものとする。

【0366】

特に、本実施の形態における暗号アルゴリズム EBF には、バージョン番号を
BF、マスター鍵としての秘密鍵を d_C 、この秘密鍵に対応する公開鍵を Q_C とし
、暗号アルゴリズム EBF に対応させて格納し、同様に本実施例の暗号アルゴリ
ズム EANG には、バージョン番号を BG、マスター鍵としての秘密鍵を d_{cg} 、
この秘密鍵に対応する公開鍵を Q_{cg} とし、暗号アルゴリズム EANG に対応させ
て格納するものとする。

【0367】

2: ネットワーク鍵管理 DB

各ユーザ、すなわち IC カード及び情報処理装置としての読取り機のユーザ ID
を $ID[1]$, $ID[2]$, ..., $ID[M]$ とし、このユーザが使用する暗号
アルゴリズムのバージョン番号を、 $V_{BP}[1]$, $V_{BP}[2]$, ..., $V_{BP}[M]$ と
し、この暗号アルゴリズムで各ユーザが使用する公開鍵を、 $Q_{ID}[1]$, $Q_{ID}[2]$, ..., $Q_{ID}[M]$ とし、各々をユーザ ID に対応させて格納するものとする。

【0368】

各ユーザが暗号アルゴリズムにあわせて使用するマスター鍵としての秘密鍵 $d_{ID}[1]$, $d_{ID}[2]$, ..., $d_{ID}[M]$ は、鍵回復機能を持たせ、各ユーザ ID に対応させて格納するものとする。

【0369】

(2) 送信側ユーザ（情報処理装置としての読取り機）の DB について

1: 暗号アルゴリズム DB

(i) このユーザが運用している暗号アルゴリズムの情報として

暗号アルゴリズム EANG、バージョン番号 BG、この暗号アルゴリズムのも
とで鍵管理用ワークステーションが使用している公開鍵 Q_{cg} 、及び、暗号アルゴ

リズムEANGに対する鍵管理用ワークステーションの署名データ S_{dcg} (EANG)を格納するものとする。

【0370】

ここで、署名データ S_{dcg} (EANG)は、暗号アルゴリズムEANGのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_{cg} で暗号アルゴリズムEANGに対して署名作成演算を実施したものである。

【0371】

(ii) ネットワーク通信システムに運用されている暗号アルゴリズムの情報として、

暗号アルゴリズム $A[1]$, $A[2]$, ..., $A[N]$ 、対応するバージョン番号 $V_B[1]$, $V_B[2]$, ..., $V_B[N]$ 、鍵管理用ワークステーションが使用する公開鍵 $Q_C[1]$, $Q_C[2]$, ..., $Q_C[N]$ 及び公開鍵 Q_{cg} に対する鍵管理用ワークステーションの署名データ $S_{dc}[1](Q_{cg})$, $S_{dc}[2](Q_{cg})$, ..., $S_{dc}[N](Q_{cg})$ をそれぞれ暗号アルゴリズムに対応させて格納するものとする。

【0372】

ここで、署名データ $S_{dc}[i](Q_{cg})$ は、暗号アルゴリズム $A[i]$ のもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 $d_C[i]$ で公開鍵 Q_{cg} に対して署名作成演算を実施したものである。

【0373】

特に、本実施例の暗号アルゴリズムEBFには、バージョン番号をBF、公開鍵 Q_C 及び、署名データ $S_{dc}(Q_{cg})$ が暗号アルゴリズムEBFに対応させて格納している。

【0374】

ここで、署名データ $S_{dc}(Q_{cg})$ は、暗号アルゴリズムEBFのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_C で公開鍵 Q_{cg} に対して署名作成演算を実施したものである。

【0375】

2: 鍵構成管理DB

ユーザが運用する暗号アルゴリズム、すなわち本実施の形態では、暗号アルゴリズム $EANG$ のもとでユーザが使用するスター鍵としての秘密鍵 d_{ID} とこの秘密鍵に対応する公開鍵 Q_{ID} 及びこの暗号アルゴリズム $EANG$ のもとで、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_{cg} で公開鍵 Q_{ID} に対して署名作成演算を実施することによって得られた署名データ $S_{dcg}(Q_{ID})$ を格納するものとする。

【0376】

(3) 受信側ユーザ (ICカード) のDBについて

1: 暗号アルゴリズムDB

このユーザが運用している暗号アルゴリズムの情報として暗号アルゴリズム EBF 、バージョン番号 BF 、この暗号アルゴリズムのもとで鍵管理用ワークステーションが使用している公開鍵 Q_c 及び、暗号アルゴリズム EBF に対する鍵管理用ワークステーションの署名データ $S_{dc}(EBF)$ を格納するものとする。

【0377】

ここで、署名データ $S_{dc}(EBF)$ は、暗号アルゴリズム EBF のもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_c で暗号アルゴリズム EBF に対して署名作成演算を実施したものである。

【0378】

2: 鍵構成管理DB

ユーザが運用する暗号アルゴリズム、すなわち本実施例では、暗号アルゴリズム EBF のもとでユーザが使用するスター鍵としての秘密鍵 d_{YID} とこの秘密鍵に対応する公開鍵 Q_{YID} 及びこの暗号アルゴリズム EBF のもとで、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_c で公開鍵 Q_{YID} に対して署名作成演算を実施することによって得られた署名データ $S_{dc}(Q_{YID})$ を格納するものとする。

【0379】

以上、暗号アルゴリズム変換の前提条件となる、鍵と暗号アルゴリズムに関するDBについて示した。

【0380】

送信側ユーザ、及び受信側ユーザのDB（データベース）には、鍵管理用ワークステーションが使用する公開鍵、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵で作成された署名データ、及び、暗号アルゴリズムとこれに対応するバージョン番号が格納されている。

【0381】

これらのデータは、すべて鍵管理用ワークステーションが配布するものとする。

【0382】

次に、図17及び図18を参照し、送信側ユーザ（情報処理装置としての読取り機）及び、受信側ユーザ（ICカード）間で実施される暗号アルゴリズム変換の形態について説明する。

【0383】

暗号アルゴリズム変換に際して、楕円曲線の暗号アルゴリズムは公開して送付することも可能であるが、本実施例では、暗号化して送付するものとして説明する。

【0384】

ここでは、前にも述べたように鍵長がEBFよりEANGのほうが長いものとし、ICカードの暗号アルゴリズムEBFを暗号アルゴリズムEANGに変換する場合の実施形態について示すこととする。

【0385】

1： ICカードを所有しているユーザは、店舗等で買い物を実施し、物品に対する支払いを行うため、ICカードを情報処理装置としての読取り機に差し込む。

【0386】

情報処理装置としての読取り機の暗号化通信管理機能は、運用している暗号アルゴリズムEANGに、バージョン番号BGを付加して＜セッション鍵発行要求＞をICカードの暗号化通信管理機能に送付する。

【0387】

2: ICカードの運用している暗号アルゴリズムのバージョン番号が、BGと一致すれば、ICカードは、自分の所有している公開鍵とこの公開鍵の署名データの発行を実施し、図21に示す手順に従って情報処理装置としての読取り機との間で暗号化通信を実施する。

【0388】

しかし、ICカードの運用している暗号アルゴリズムEBFのバージョン番号は、BFであり、送付されたバージョン番号BGとは異なる。

【0389】

バージョン番号が異なると判断した暗号化通信管理機能は、このバージョン番号はBFを付加して、＜暗号アルゴリズム更新要求＞を情報処理装置としての読取り機の暗号化通信管理機能に返送する。

【0390】

3: 情報処理装置としての読取り機は、バージョン番号はBFをもとに暗号アルゴリズムDBを検索し、暗号アルゴリズムEANGで運用する鍵管理用ワークステーションの公開鍵 Q_{cg} 及び、暗号アルゴリズムEBFのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_c で公開鍵 Q_{cg} に対して署名作成演算を実施して得られた署名データ $S_{dc}(Q_{cg})$ とを取り出し、この公開鍵 Q_{cg} と署名データ $S_{dc}(Q_{cg})$ をICカードに送付する。

【0391】

4: ICカードは、暗号アルゴリズムEBFのもとに運用する鍵管理用ワークステーションの公開鍵 Q_c を用いて、送付された公開鍵 Q_{cg} と署名データ $S_{dc}(Q_{cg})$ に対して署名検証演算を実施し、公開鍵 Q_{cg} が正当な情報処理装置としての読取り機から送付されたものであることを確認する。

【0392】

5: 次に、ICカードは、鍵構成管理DBから暗号アルゴリズムEBFで運用するICカードの公開鍵 Q_{YID} 及び、暗号アルゴリズムEBFのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_c で公開鍵 Q_{YID} に対して署名作成演算を実施し、管理用ワークステーションから配布された署名デ

ータ $S_{dc}(Q_{YID})$ とを取り出し、この公開鍵 Q_{YID} と署名データ $S_{dc}(Q_{YID})$ とを情報処理装置としての読取り機に送付する。

【0393】

6： 情報処理装置としての読取り機は、暗号アルゴリズム EBF のもとに運用する鍵管理用ワークステーションの公開鍵 Q_c を用いて、送付された公開鍵 Q_{YID} と署名データ $S_{dc}(Q_{YID})$ に対して署名検証演算を実施し、公開鍵 Q_{YID} が正当な IC カードから送付されたものであることを確認する。

【0394】

7： 情報処理装置としての読取り機は、暗号アルゴリズム EANG を送付された公開鍵 Q_{YID} で暗号アルゴリズム EBF を運用して暗号化し、暗号文 $EBF_{Q_{YID}}(EANG)$ を作成する。

【0395】

これと併せて、暗号アルゴリズム EANG のもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵 d_{cg} で暗号アルゴリズム EANG に対して署名作成演算を実施し管理用ワークステーションから配布された署名データ $S_{dcg}(EANG)$ を取り出し、暗号文 $EBF_{Q_{YID}}(EANG)$ と署名データ $S_{dcg}(EANG)$ とを、IC カードに送付する。

【0396】

8： IC カードは、暗号アルゴリズム EBF で運用する IC カード所有の秘密鍵 d_{YID} を用いて送付された暗号文 $EBF_{Q_{YID}}(EANG)$ を復号化し、暗号アルゴリズム EANG を取得する。

【0397】

次に、IC カードは、運用する暗号アルゴリズムを EBF から取得した EANG に変換し、4：項で取得した鍵管理ワークステーションの公開鍵 Q_{cg} を用いて、取得した暗号アルゴリズム EANG と送付された署名データ $S_{dcg}(EANG)$ に対して、署名検証演算を実施し、正当な情報処理装置としての読取り機から配布された暗号アルゴリズムであることを確認する。これにより、暗号アルゴリズムをこの EANG への更新を完了する。

【0398】

9： 暗号アルゴリズムEANGの鍵長は、暗号アルゴリズムEBFより長い
ため、ICカードのマスター鍵としての秘密鍵 d_{YID} は、そのまま暗号アルゴリ
ズムEANGの秘密鍵として使用することとし、送付された暗号アルゴリズム
EANGのベースポイントPより、対応する公開鍵 Q_{YIDC} ($= P \cdot d_{YID}$; \cdot は
楕円曲線上の演算)を生成する。

【0399】

ICカードは、暗号アルゴリズムを一旦EBFに戻し、この暗号アルゴリズム
EBFのもとに公開鍵 Q_{YIDC} に対して秘密鍵 d_{YID} を用いて署名作成演算を実施
し、署名データ $S_{dYID}(Q_{YIDC})$ を作成する。

【0400】

ICカードは、生成した公開鍵 Q_{YIDC} 及び署名データ $S_{dYID}(Q_{YIDC})$ とを、
情報処理装置としての読取り機に送付する。

【0401】

10： 情報処理装置としての読取り機は、暗号アルゴリズムを一旦EBFに
変換し、6：項で取得した公開鍵 Q_{YID} を用いて、送付された署名データ S_{dYID}
(Q_{YIDC})と公開鍵 Q_{YIDC} に対して署名検証演算を実施し、正当なICカードか
ら配布されたICカードの公開鍵 Q_{YIDC} であることを確認する。

【0402】

この後、暗号アルゴリズムを再度暗号アルゴリズムEANGに変換する。

【0403】

11： 情報処理装置としての読取り機は、鍵構成管理DBから暗号アルゴリ
ズムEANGで運用する情報処理装置としての読取り機の使用する公開鍵 Q_{ID} 及
び、暗号アルゴリズムEANGのもとに鍵管理用ワークステーションが使用する
マスター鍵としての秘密鍵 d_{cg} で公開鍵 Q_{ID} に対して署名作成演算を実施し、管
理用ワークステーションから配布された署名データ $S_{dcg}(Q_{ID})$ とを取り出し
、この公開鍵 Q_{ID} と署名データ $S_{dcg}(Q_{ID})$ とをICカードに送付する。

【0404】

12： ICカードは、暗号アルゴリズムEANGのもと4：項で取得した鍵

管理用ワークステーションの公開鍵 Q_{cg} を用いて、送付された署名データ S_{dcg} (Q_{ID}) と公開鍵 Q_{ID} に対して署名検証演算を実施し、正当な情報処理装置としての読取り機から送付された情報処理装置としての読取り機の公開鍵 Q_{ID} であることを確認する。

【0405】

13: 以上により、ICカードと情報処理装置としての読取り機は、暗号アルゴリズムEANGを共有し、お互いの公開鍵（情報処理装置としての読取り機の公開鍵 Q_{ID} 、及び、ICカードの公開鍵 Q_{YIDC} ）の正当性を確認した。データの暗号化をこの公開鍵で実施することにすれば、ICカードと情報処理装置としての読取り機との間で暗号化通信及び、署名作成演算、署名検証演算を実施することができ、支払いなどの決済が実施可能となった。

【0406】

ここで、上述した実施手順において、鍵管理用ワークステーションは一切関与していない。

【0407】

ただし、ICカードは、変換した公開鍵 Q_{YIDC} について、鍵管理用ワークステーションの署名データを所有していないため、これをそのまま使用することはできず、支払いなどの決済が終了したあと、暗号アルゴリズムをEANGからEBFに戻す必要がある。

【0408】

次に、図18を参照し、ICカードの変換した公開鍵 Q_{YIDC} について、鍵管理用ワークステーションの署名データを取得する実施形態について説明する。

【0409】

1: 情報処理装置としての読取り機は、正当性を確認した暗号アルゴリズムEANGで運用するICカードの公開鍵 Q_{YIDC} に対して、暗号アルゴリズムEBFのもとに秘密鍵 d_{YID} を用いて作成した署名データ S_{dYID} (Q_{YIDC}) をICカードから送られている。

【0410】

この署名データ S_{dYID} (Q_{YIDC}) と公開鍵 Q_{YIDC} 、及び暗号アルゴリズムEBF

Fで運用するICカードの公開鍵 Q_{YID} 、暗号アルゴリズムEBFのバージョン番号BF、暗号アルゴリズムEANGのバージョン番号BG及びICカードのユーザIDとを鍵管理用ワークステーションに送付する。

【0411】

2： 鍵管理用ワークステーションは、まずICカードのユーザIDをキーとして、ネットワーク鍵管理DBを検索し、送付されたICカードの公開鍵 Q_{YID} が存在することを確認する。

【0412】

ICカードの公開鍵 Q_{YID} を用いて、署名データ $S_{dYID}(Q_{YIDC})$ と公開鍵 Q_{YIDC} に対して署名検証演算を実施し公開鍵 Q_{YIDC} が正当なICカードのものであることを確認する。

【0413】

以上により、公開鍵 Q_{YIDC} が、ICカードの公開鍵であることを確認した。

【0414】

3： この公開鍵 Q_{YIDC} に対して、暗号アルゴリズムEANGで運用する鍵管理用ワークステーションの秘密鍵 d_{cg} を用いて、署名作成演算を実施し、署名データ $S_{dcg}(Q_{YIDC})$ を作成し、情報処理装置としての読取り機に返送する。

【0415】

また、鍵管理用ワークステーションは、ネットワーク鍵管理DBのICカードのユーザIDに対応させて格納している暗号アルゴリズムのバージョン番号及び公開鍵を、それぞれBG及び Q_{YIDC} に更新する。

【0416】

4： 情報処理装置としての読取り機は、この署名データ $S_{dcg}(Q_{YIDC})$ をICカードに転送する。

【0417】

以上の処理を実施すれば、ICカードは、公開鍵 Q_{YIDC} に対して鍵管理用ワークステーションの署名データ $S_{dcg}(Q_{YIDC})$ を取得することができる。

【0418】

上述した実施の形態において、鍵管理用ワークステーションは、変換前の公開

鍵 Q_{YID} の存在と、変換後の公開鍵 Q_{YIDC} の署名データを確認しており、ICカードの成りすましを防止することができる。

【0419】

このようにして、ICカードは暗号アルゴリズムEANGで運用する公開鍵 Q_{YIDC} と、鍵管理用ワークステーションの署名データ $S_{dcg}(Q_{YIDC})$ とを所有し、以降暗号アルゴリズムEANGを運用することが、可能となった。

【0420】

鍵管理用ワークステーションの関与は、変換した暗号アルゴリズムに対して生成された公開鍵について署名作成及び、署名検証演算の実施するだけであり、以上の方法によりICカードを情報処理装置としての読取り機にさし込んだまま、暗号アルゴリズム変換を実施することができる。

【0421】

ここで示した、暗号アルゴリズム変換では、新しい暗号アルゴリズムに対して、ユーザ（ここではICカード）は自分の所有する秘密鍵と公開鍵とを自ら生成している。

【0422】

ここで示した実施形態では、変換前の暗号アルゴリズムと変換後の暗号アルゴリズムに対して、ユーザの所有する秘密鍵を同一となるように定めている。

【0423】

このような秘密鍵の設定の方式は、システムに混在する複数の暗号アルゴリズムの鍵長がまちまちで、どのユーザがどの鍵長の暗号アルゴリズムを使用しているか特定できないときに有効である。

【0424】

これに対して、暗号アルゴリズム変換をすべてのユーザが使用していない、別の長い鍵長への変換を考える。

【0425】

この場合、各ユーザが使用する秘密鍵の鍵長を変換前のものと同じ鍵長で使ったとすれば、暗号アルゴリズムの許容する鍵長が折角長くなったにもかかわらず、すべてのユーザの使用している鍵長は増加していない。この場合、暗号アタ

ックするほうでは、アタックする鍵長の範囲をもとの鍵長に限定して攻撃することも可能である。これでは、暗号アルゴリズムの許容する鍵長を折角長くとっても実質的に暗号強度を増加させたことにならない。

【0426】

このような事態を回避するためには、前述の図15に示したような鍵長を長くする方法が有効と考えられる。

【0427】

この場合、すべてのユーザは任意に乱数に基づいて鍵長を付加しても、同じものが存在しないため、鍵の管理が容易になるものと考えられる。

【0428】

新しく、システムに参加するユーザに対してのみ同一の鍵が存在しないように配慮すれば良い。

【0429】

ここで示した、新しい暗号アルゴリズムに対して、ユーザが自分の所有する秘密鍵と公開鍵とを自ら生成する方法は、前述の図13、図14、図11で述べた通常の暗号アルゴリズム変換に対しても適用可能である。ユーザが自分の所有する秘密鍵を生成すれば、鍵管理用ワークステーションから解読される可能性を回避することができる。以下、図20を参照して、暗号アルゴリズム変換に対してユーザが自分の所有する秘密鍵を生成する形態について説明する。

【0430】

この場合の暗号アルゴリズム変換においても、スクランブル機能、デスクランブル機能などを確認する必要があるが、これは、図13、図14、図11で述べた方法と全く同じであるため、ここでは暗号アルゴリズムの配信とユーザが自分の所有する秘密鍵を生成する方法に限定して述べることにする。

【0431】

ここで述べる公開鍵暗号方式の運用形態は、図16に示す暗号化通信方式をとるものとし、図20はこの暗号化通信方式において、暗号アルゴリズム変換の実施形態を示したものである。

【0432】

この図において、受信側ユーザの運用している暗号アルゴリズムをEBFとし、変換する暗号アルゴリズムをEANGとする。

【0433】

図13、図14、図11で述べた時と同じように、鍵管理用ワークステーションが暗号アルゴリズムEBFに対して運用するマスター鍵としての秘密鍵を d_c とし、この秘密鍵に対応する公開鍵を Q_c とする。

【0434】

同様に、暗号アルゴリズムをEANG対して鍵管理用ワークステーションが運用するマスター鍵としての秘密鍵を d_{cg} とし、この秘密鍵に対応する公開鍵を Q_{cg} とする。

【0435】

一方、受信側ユーザが暗号アルゴリズムEBFに対して、運用するマスター鍵としての秘密鍵を d_{YID} とし、この秘密鍵に対応する公開鍵を Q_{YID} とする。

【0436】

以上の前提条件は、図13、14、11で示したものと同一であり、以下暗号アルゴリズム変換の実施形態について説明する。

【0437】

(1) 鍵管理用ワークステーションのネットワーク鍵管理機能は、変換前の暗号アルゴリズムEBFを使用して、以下の暗号文及び、署名データを作成する。

【0438】

1: 変換前の暗号アルゴリズムEBFで暗号アルゴリズムEANGを暗号化するためのスクランブル鍵 K_{SB} 、復号化するためのデスクランブル鍵 K_{DB} を生成する。

【0439】

2: 暗号アルゴリズムEANGをスクランブル鍵 k_{SB} で暗号化し、暗号文 $E_{BF_{KSB}}(EANG)$ を作成する。

【0440】

また、受信側ユーザのマスター鍵としての公開鍵 Q_{YID} を取りだし、デスクラ

ンブル鍵 K_{DB} を暗号化し、暗号文 $E B F_{QYID}(K_{DB})$ を作成する。

【0441】

3: 変換前の暗号アルゴリズム $E B F$ と鍵管理用ワークステーションのマスター鍵である秘密鍵 d_c で、暗号アルゴリズム $E A N G$ に対し署名作成演算を実施し、署名データ $S_{dc}(E A N G)$ を作成する。

【0442】

4: 変換前の暗号アルゴリズム $E B F$ と鍵管理用ワークステーションのマスター鍵である秘密鍵 d_c で変換後の暗号アルゴリズム $E A N G$ に適用する鍵管理用ワークステーションのマスター鍵としての公開鍵 Q_{cg} に対して署名作成演算を実施し、署名データ $S_{dc}(Q_{cg})$ を作成する。

【0443】

5: 作成した2組の暗号文 $E B F_{QYID}(K_{DB})$ 、 $E B F_{KSB}(E A N G)$ 、と2組の署名データ $S_{dc}(E A N G)$ 、 $S_{dc}(Q_{CG})$ 及び、鍵管理用ワークステーションの公開鍵 Q_{cg} を受信側ユーザに送付する。

【0444】

(2) 受信側ユーザの暗号アルゴリズムの取得

受信側ユーザは、暗号アルゴリズムとして $E B F$ を運用しており、マスター鍵としての秘密鍵 d_{YID} 、及び暗号アルゴリズム $E B F$ で運用される鍵管理用ワークステーションの公開鍵 Q_C を所有している。

【0445】

鍵管理用ワークステーションより送付された暗号文から

1: マスター鍵として秘密鍵 d_{YID} を用いて、暗号文 $E B F_{QYID}(K_{DB})$ を復号し、デスクランブル鍵 K_{DB} を取得する。次にこのデスクランブル鍵 K_{DB} を用いて暗号文 $E B F_{KSB}(E A N G)$ を復号し、暗号アルゴリズム $E A N G$ を取得する。

【0446】

暗号アルゴリズム $E B F$ において、鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(E A N G)$ と取得した暗号アルゴリズム $E A N G$ に対して署名検証演算を実施し、取得した暗号アルゴリズム $E A N G$ が正当な鍵管

理用ワークステーションから送付されたものであることを確認する。

【0447】

2: 暗号アルゴリズム EBF において、鍵管理用ワークステーションの公開鍵 Q_C を用いて、署名データ $S_{dc}(Q_{cg})$ と送付された鍵管理用ワークステーションの変換した暗号アルゴリズム EANG 上で運用する公開鍵 Q_{cg} に対して署名検証演算を実施し、送付された公開鍵が正当な鍵管理用ワークステーションの公開鍵であることを確認する。

【0448】

以上のようにして、受信側ユーザは、暗号アルゴリズム EANG 及び、鍵管理用ワークステーションの暗号アルゴリズム EANG 上で運用する公開鍵 Q_{cg} 取得した。これより、取得した暗号アルゴリズム EANG を暗号アルゴリズム管理 DB に登録するとともに、暗号アルゴリズム管理機能により運用する暗号アルゴリズムを EBF だけでなく EANG も運用可能となった。

【0449】

(3) 受信側ユーザの所有する鍵の変換

1: 鍵管理用ワークステーションより送付された暗号アルゴリズム EANG に対して、受信側ユーザは新規に自ら所有するマスター鍵としての秘密鍵 d_{YIDC} を新規に生成する。

【0450】

秘密鍵を生成するための方法として、次の 3 つが挙げられる。

【0451】

(a) 暗号アルゴリズム EBF で運用している秘密鍵 d_{YID} を暗号アルゴリズム EANG の秘密鍵として使用する。

【0452】

(b) 図 15 で示したように、暗号アルゴリズム EBF で運用している秘密鍵 d_{YID} に乱数を付加して秘密鍵 d_{YIDC} を新規に生成する。

【0453】

(c) 暗号アルゴリズム EANG の情報により、まったく新規に秘密鍵 d_{YIDC} を生成する。

【0454】

これらのうちのいずれかの方法で、受信側ユーザ自ら所有する秘密鍵 d_{YIDC} を生成し、この秘密鍵に対応する公開鍵 Q_{YIDC} を生成する。

【0455】

ここで、前記(c)の方法は、先に述べたように他のユーザの使用する鍵と一致する可能性もあるので、鍵管理用ワークステーションにより、他のユーザの使用する公開鍵がないことを確認する必要がある。

【0456】

変換する暗号アルゴリズム $EANG$ が楕円曲線暗号の場合、このアルゴリズムのベースポイントを P として、公開鍵 Q_{YIDC} は、 $P \cdot d_{YIDC}$ (\cdot は楕円曲線上の演算) で与えられる。

【0457】

2: 受信側ユーザは一旦暗号アルゴリズムを EBF に戻し、この暗号アルゴリズム EBF のもとに公開鍵 Q_{YIDC} に対して秘密鍵 d_{YID} を用いて署名作成演算を実施し、署名データ $S_{dYID}(Q_{YIDC})$ を作成し、生成した公開鍵 Q_{YIDC} 、署名データ $S_{dYID}(Q_{YIDC})$ 及び受信側ユーザのユーザ ID とを、鍵管理用ワークステーションに送付する。

【0458】

3: 鍵管理用ワークステーションは、暗号アルゴリズムを EBF に戻し、送付されたユーザ ID をキーとしてネットワーク鍵管理 DB を検索し、当該受信側ユーザの公開鍵 Q_{YID} を取り出す。次に、この受信側ユーザの公開鍵 Q_{YID} を用いて、送付された公開鍵 Q_{YIDC} 及び署名データ $S_{dYID}(Q_{YIDC})$ に対して署名検証演算を実施し、正当な受信側ユーザから送付された公開鍵 Q_{YIDC} であることを確認する。

【0459】

鍵管理用ワークステーションは、ネットワーク鍵管理 DB を検索し、受信側ユーザの公開鍵 Q_{YID} を確認しているため、受信側ユーザの成りすましを防止することができる。

【0460】

以上により鍵管理用ワークステーションは、変換した暗号アルゴリズムEANGにおいて、受信側ユーザが運用する公開鍵 Q_{YIDC} を取得した。以降、鍵管理用ワークステーションは、暗号アルゴリズムEANGで運用するマスター鍵としての秘密鍵 d_{cg} を用いて、受信側ユーザが運用する公開鍵 Q_{YIDC} に署名作成演算を実施し、署名データ $S_{dcg}(Q_{YIDC})$ を作成し受信側ユーザに送付すること、及び、スクランブル機能、デスクランブル機能を確認するなど、一連の暗号アルゴリズム変換に関する手続きが必要となるが、これらは、図13、図14、図11で述べた暗号アルゴリズム変換に関する手続きで実施すればよい。

【0461】

以上、新しい暗号アルゴリズムに対して、ユーザが自分の所有する鍵を自ら生成する実施の形態について説明した。

【0462】

最後に、

- (1) 共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの変換
 - (2) 公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの変換
- について説明する。

【0463】

- (1) 共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの変換について

図8、9、6に共通鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの暗号アルゴリズム変換の実施形態について説明した。

【0464】

この場合、変換前の暗号アルゴリズムをEBFとし、変換後の暗号アルゴリズムをEANGとしている。

【0465】

共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの暗号アルゴリズム変換を実施する場合、この記号にあわせて変換前の共通鍵暗号アルゴリズムをEBFとし、変換後の公開鍵暗号アルゴリズムをEANGとして説明を行う。

【0466】

変換後の公開鍵暗号アルゴリズムEANGは、図8、9、6に示す実施形態に従って、変換前の共通鍵暗号アルゴリズムEBFで暗号化して、配信することができる。

【0467】

公開鍵暗号アルゴリズムへ変換する場合、新規に秘密鍵と公開鍵とを生成し、変換した公開鍵暗号アルゴリズムに対して、スクランブル機能、デスクランブル機能を確認する必要があるが、この一連の鍵生成と機能確認は、図13、14、11で示した公開鍵暗号アルゴリズムの変換の実施形態に従って、実施することができる。

【0468】

(2) 公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの変換について

共通鍵暗号アルゴリズムは、公開鍵暗号アルゴリズムと比較すると署名作成、署名検証の演算がない点異なる。

【0469】

従って、公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する場合、図13、14、11で示した公開鍵暗号アルゴリズムの変換の実施形態において、この署名作成及び署名検証の演算を除いた手順で、暗号アルゴリズムの変換を実施することができる。

【0470】

以上で、暗号アルゴリズム変換の実施形態について示した。

【0471】

図5に示した暗号アルゴリズム変換の実施形態の概要、図8、9、6に示した共通鍵暗号アルゴリズム変換の実施形態、及び、図13、14、11で示した公開鍵暗号アルゴリズムの変換の実施形態において、暗号アルゴリズム変換が正常に実施できたかどうかは、暗号化通信システムのスクランブル機能、デスクランブル機能を動作させ、それぞれ平文データMDとして<アルゴリズム変換後のデスクランブル機能確認終了>及び、平文データMSとして<アルゴリズム変換確

認試験終了>を暗号化して送付し、復号されるかどうかで確認している。

【0472】

この暗号アルゴリズム変換確認のそれぞれのプロセスにおいて、所要の平文データMD、または平文データMSが復号されなかった場合は、<暗号アルゴリズム変換動作異常>の応答メッセージを送信し、当該プロセスを再度、実行するものとする。

【0473】

図17、18および図13、14、11で示した公開鍵暗号アルゴリズム変換の実施形態における暗号アルゴリズム変換のデータのやり取りのプロセスにおいて、公開鍵暗号アルゴリズムでの署名作成データに対する署名検証演算を実施している。この署名検証演算を実施した結果、署名作成データに異常が発生した場合も、<暗号アルゴリズム変換動作異常>の応答メッセージを送信し、当該プロセスを再度実行するものとする。

【0474】

再実行後も平文データMDまたは平文データMSが復号されなかった場合、および、署名検証演算を実施した結果、署名作成データに異常が発生した場合も、その段階で<暗号アルゴリズム変換異常終了>の応答メッセージを送信し、暗号アルゴリズム変換プロセスを中断するものとする。

【0475】

<暗号アルゴリズム変換異常終了>の応答が発生した場合は、暗号化通信システムの構成要素を、ハード、ソフトの面から点検する作業を実施するものとする。

【0476】

図13、14、11は、公開鍵暗号アルゴリズム変換の実施形態を示しているが、暗号アルゴリズム変換を実施しない場合、すなわち、暗号アルゴリズムが同じで暗号アルゴリズムを配布しない場合は、鍵管理局からユーザの使用する鍵の更新、削除等、鍵配送の手順を与えている。図17、18で示した公開鍵暗号アルゴリズム変換の実施形態では、平文データMDおよびMSによる暗号アルゴリズム変換確認のプロセスについて記述していないが、いうまでもなく、図13、

14、11に示した実施形態にしたがって平文データMDおよびMSを当該暗号アルゴリズムの公開鍵で暗号化して送付することで、暗号アルゴリズム変換確認を実施することができる。

【0477】

【発明の効果】

本発明によれば、暗号アルゴリズムの配信を安全に、しかも、それに要する時間と手間を削減した状態で、暗号アルゴリズムを変換することができる。

【0478】

また、このような暗号アルゴリズムの変換によって、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することが可能となる。

【図面の簡単な説明】

【図1】 ネットワーク通信システムを示す説明図である。

【図2】 ネットワーク通信システムの各部の機能構成を示す機能ブロック図である。

【図3】 鍵管理用ワークステーションからアクセスされるデータベースに格納される情報を示す説明図であって、(a) ネットワーク暗号アルゴリズム管理データベースに格納される情報、(b) ネットワーク鍵管理データベースに格納される情報を示す。

【図4】 パーソナルコンピュータからアクセスされるデータベースに格納される情報を示す説明図であって、(a) 暗号アルゴリズム管理データベースに格納される情報、(b) 鍵構成管理データベースに格納される情報を示す。

【図5】 本発明を適用した暗号アルゴリズムの変換の概略を示すデータフロー図である。

【図6】 本発明を適用した、共通鍵暗号における暗号アルゴリズム変換を示すデータフロー図である。

【図7】 本発明を適用した、共通鍵暗号における暗号化通信を示すデータフロー図である。

【図 8】 本発明を適用した、共通鍵暗号における暗号アルゴリズム変換の手順の前半部を示すフロー図である。

【図 9】 本発明を適用した、共通鍵暗号における暗号アルゴリズム変換の手順の後半部を示すフロー図である。

【図 10】 本発明を適用した、共通鍵暗号における暗号鍵の変更を示す説明図であって、(a) 鍵長が短くなる場合、(b) 鍵長が短くなる場合の鍵の変更形態を示す。

【図 11】 本発明を適用した、公開鍵暗号における暗号化通信を示すデータフロー図である。

【図 12】 本発明を適用した、公開鍵暗号における暗号アルゴリズム変換を示すデータフロー図である。

【図 13】 本発明を適用した、公開鍵暗号における暗号アルゴリズム変換の手順の前半部を示すフロー図である。

【図 14】 本発明を適用した、公開鍵暗号における暗号アルゴリズム変換の手順の後半部を示すフロー図である。

【図 15】 本発明を適用した、公開鍵暗号における暗号鍵の変更を示す説明図である。

【図 16】 本発明を適用した、公開鍵暗号アルゴリズムによる暗号化通信システムを示すデータフロー図である。

【図 17】 本発明を適用した、可搬型の情報処理装置における暗号アルゴリズム変換を示すデータフロー図である。

【図 18】 本発明を適用した、可搬型の情報処理装置における、他の形態の暗号アルゴリズム変換を示すデータフロー図である。

【図 19】 本発明を適用した、暗号鍵および暗号アルゴリズムに関するデータベースを示す説明図である。

【図 20】 本発明を適用した、暗号アルゴリズム変換であって、ユーザによって暗号鍵が生成される場合を示すデータフロー図である。

【図 21】 本発明を適用した、公開鍵暗号アルゴリズムにおける暗号化通信システムを示すブロック図である。

【図 22】 ネットワーク通信システムの他の態様を示す説明図である。

【図 23】 本発明を適用した、鍵回復機能の暗号化における作用を示す説明図である。

【図 24】 本発明を適用した、鍵回復機能の復号化における作用を示す説明図である。

【図 25】 本発明を適用した、公開鍵暗号アルゴリズムによる、ICカードを用いた暗号化通信システムを示すブロック図である。

【符号の説明】

100…パーソナルコンピュータ、110…鍵構成管理機能、120…暗号アルゴリズム管理機能、130…スクランブル機能、140…デスクランブル機能、150…暗号化通信管理機能、180…鍵構成管理データベース、181…ユーザ固有鍵データベース、190…暗号アルゴリズムデータベース、200…パーソナルコンピュータ、210…鍵構成管理機能、220…暗号アルゴリズム管理機能、230…スクランブル機能、240…デスクランブル機能、250…暗号化通信管理機能、280…鍵構成管理データベース、281…ユーザ固有鍵データベース、290…暗号アルゴリズムデータベース、400…鍵管理局、500…鍵管理用ワークステーション、530…スクランブル機能、540…デスクランブル機能、550…暗号化通信管理機能、560…ネットワーク暗号アルゴリズム管理機能、570…ネットワーク鍵管理機能、580…ネットワーク鍵管理データベース、581…ユーザ固有鍵データベース、590…ネットワーク暗号アルゴリズムデータベース、595…暗号アルゴリズム生成機能、700…ICカード、710…鍵構成管理機能、720…暗号アルゴリズム管理機能、730…スクランブル機能、740…デスクランブル機能、750…暗号化通信管理機能、780…鍵構成管理データベース、790…暗号アルゴリズムデータベース。

【書類名】 図面

【図 1】

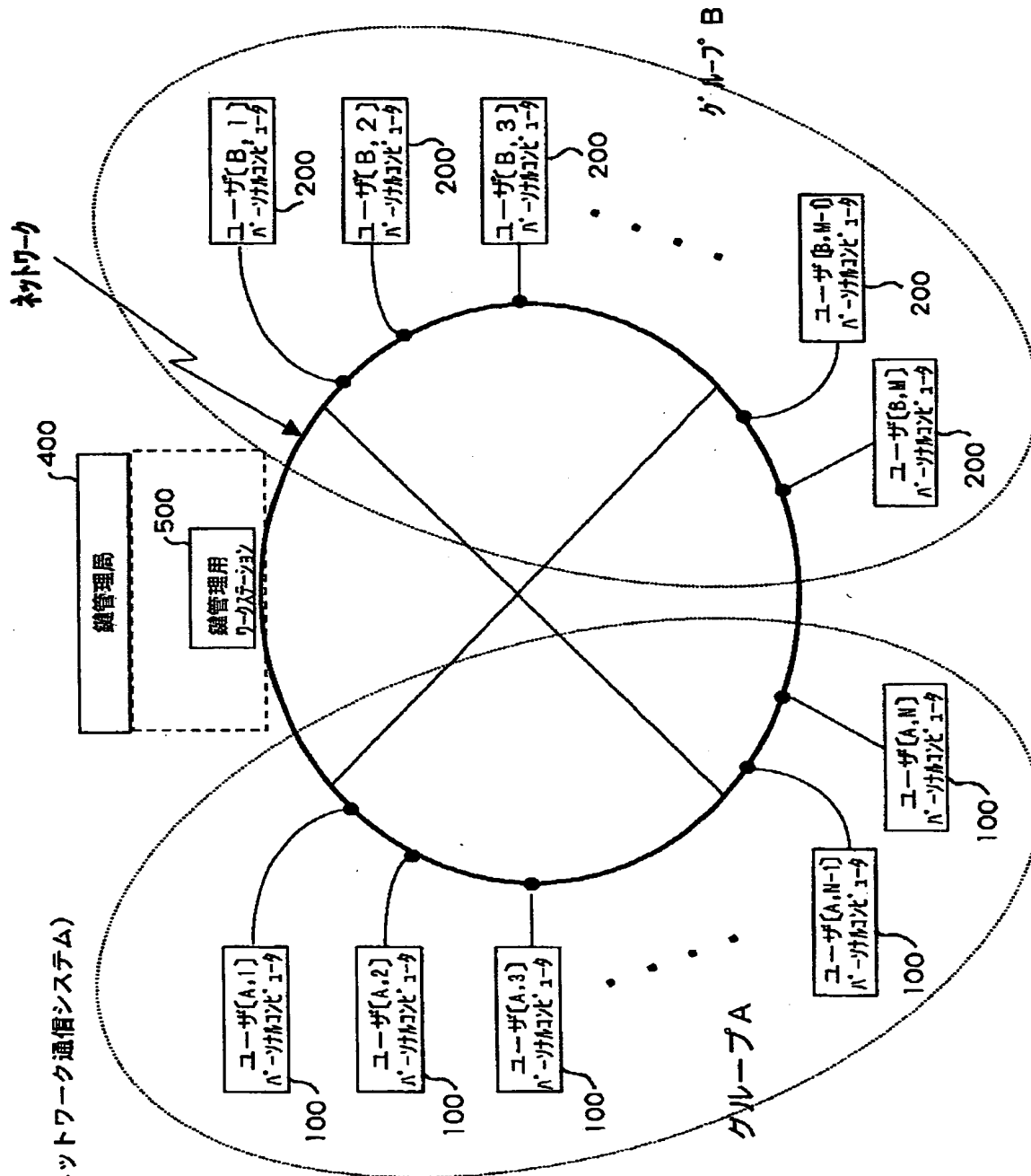
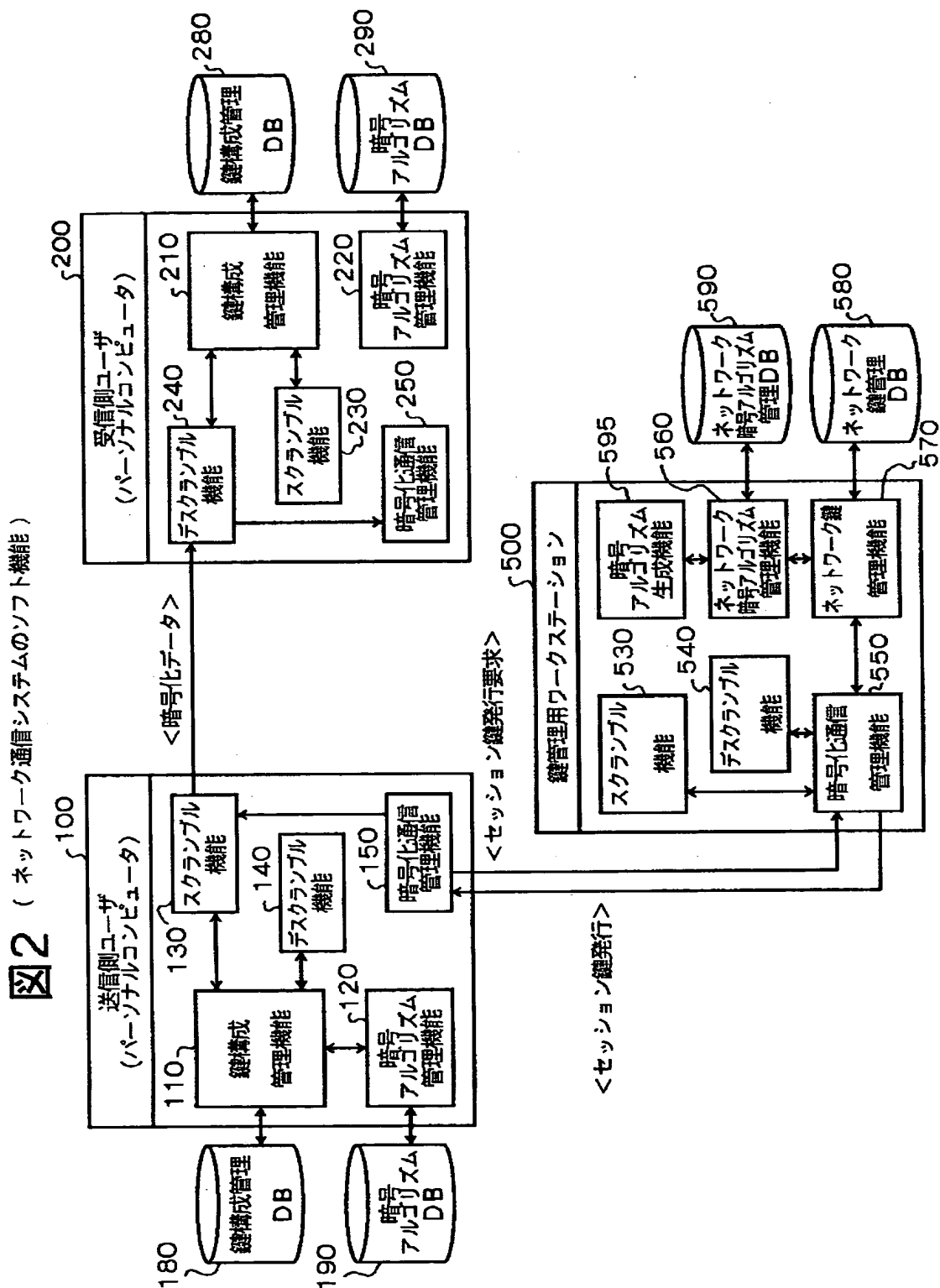


図 1 (ネットワーク通信システム)

【図 2】



【図 3】

図3

(a) ネットワーク暗号アルゴリズム管理DB

ユーザID	暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時
鍵管理局ID	暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時

(b) ネットワーク鍵管理DB

ユーザID	暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵情報	更新日時
鍵管理局ID	暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵情報	更新日時

【図 4】

図4

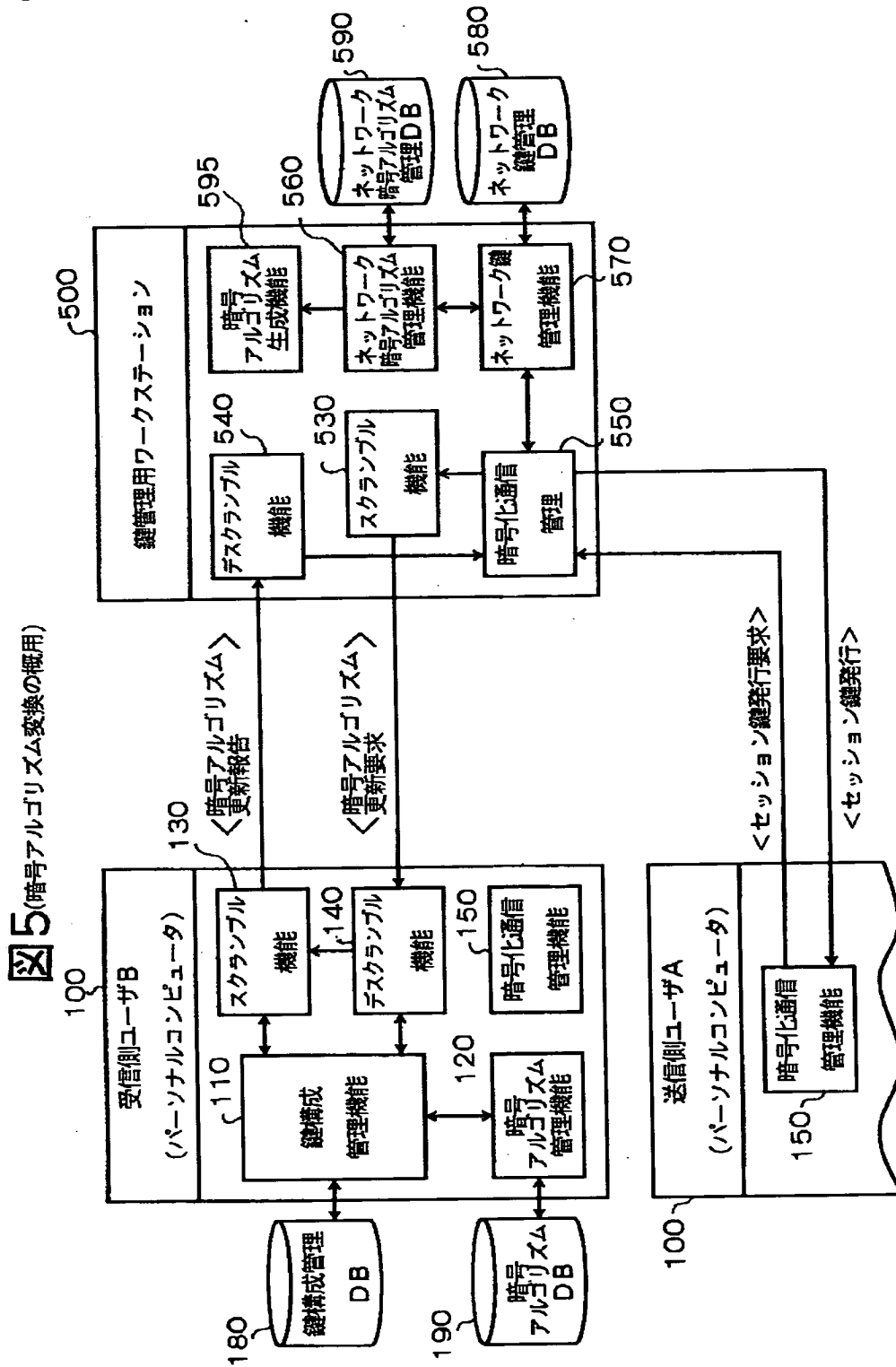
(a) 暗号アルゴリズム管理DB

暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時
-----------	---------------	------

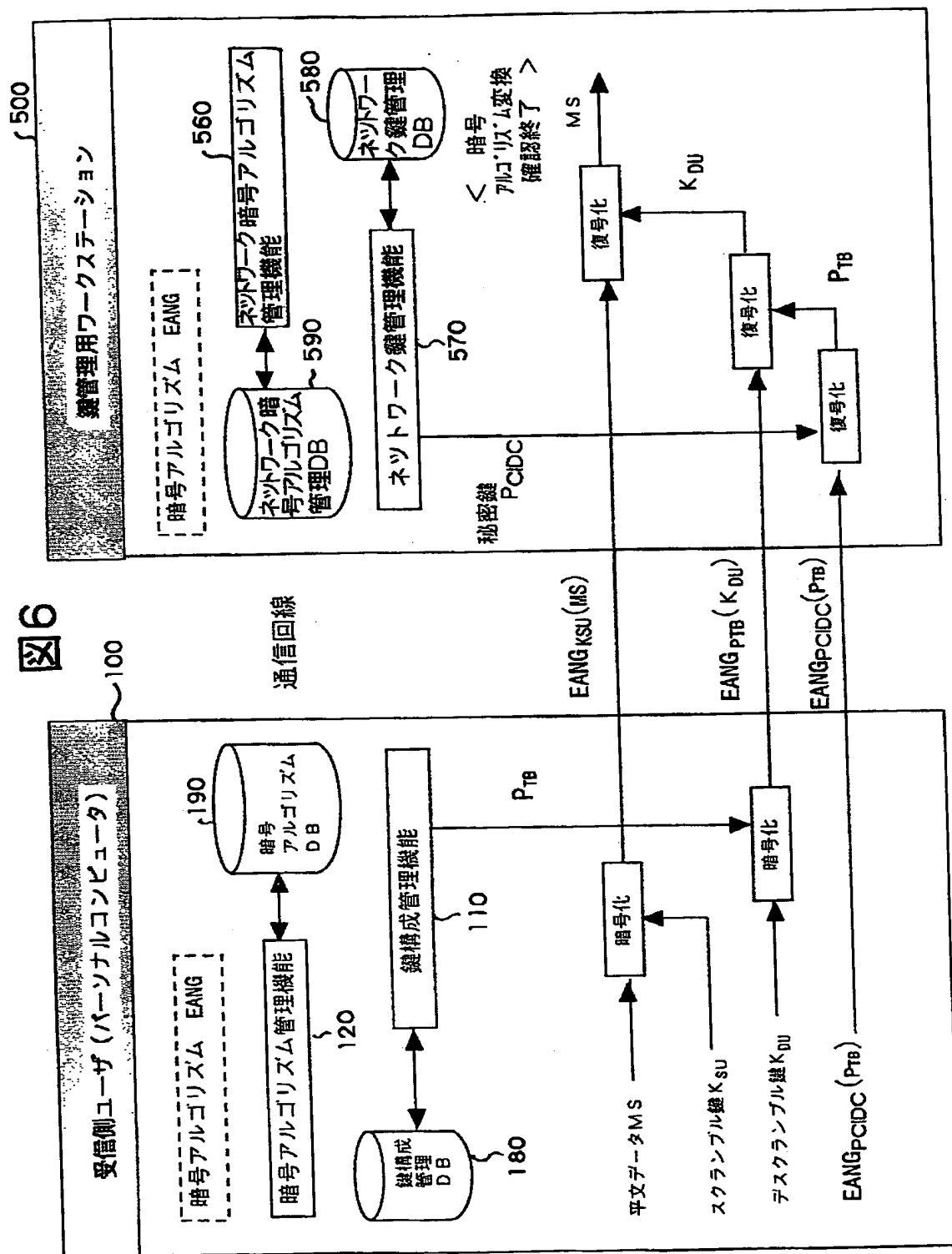
(b) 鍵構成管理DB

暗号アルゴリズム名	暗号アルゴリズムバージョン	ユーザ鍵情報	更新日時
暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵管理局の鍵情報	更新日時

【図5】

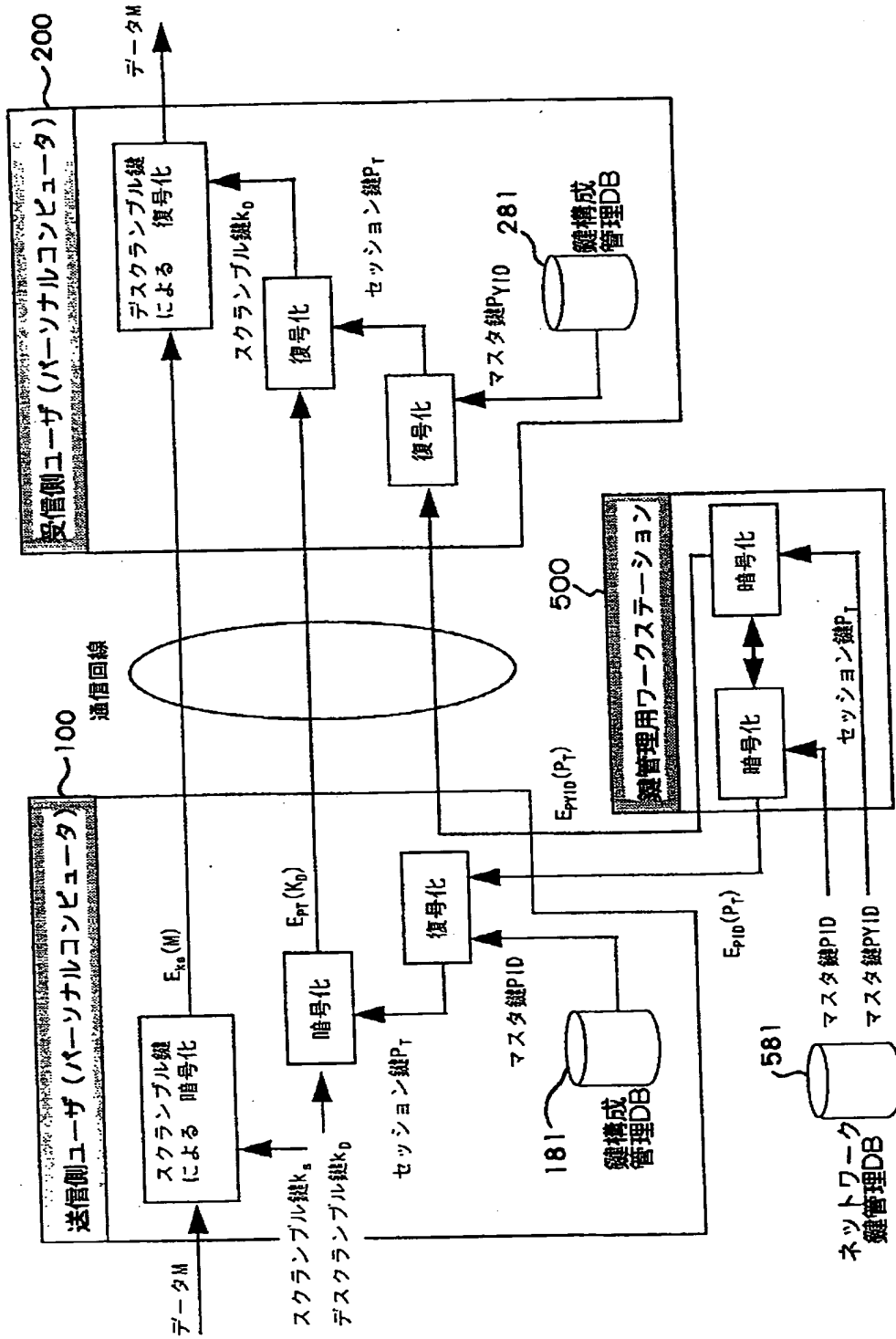


【圖 6】



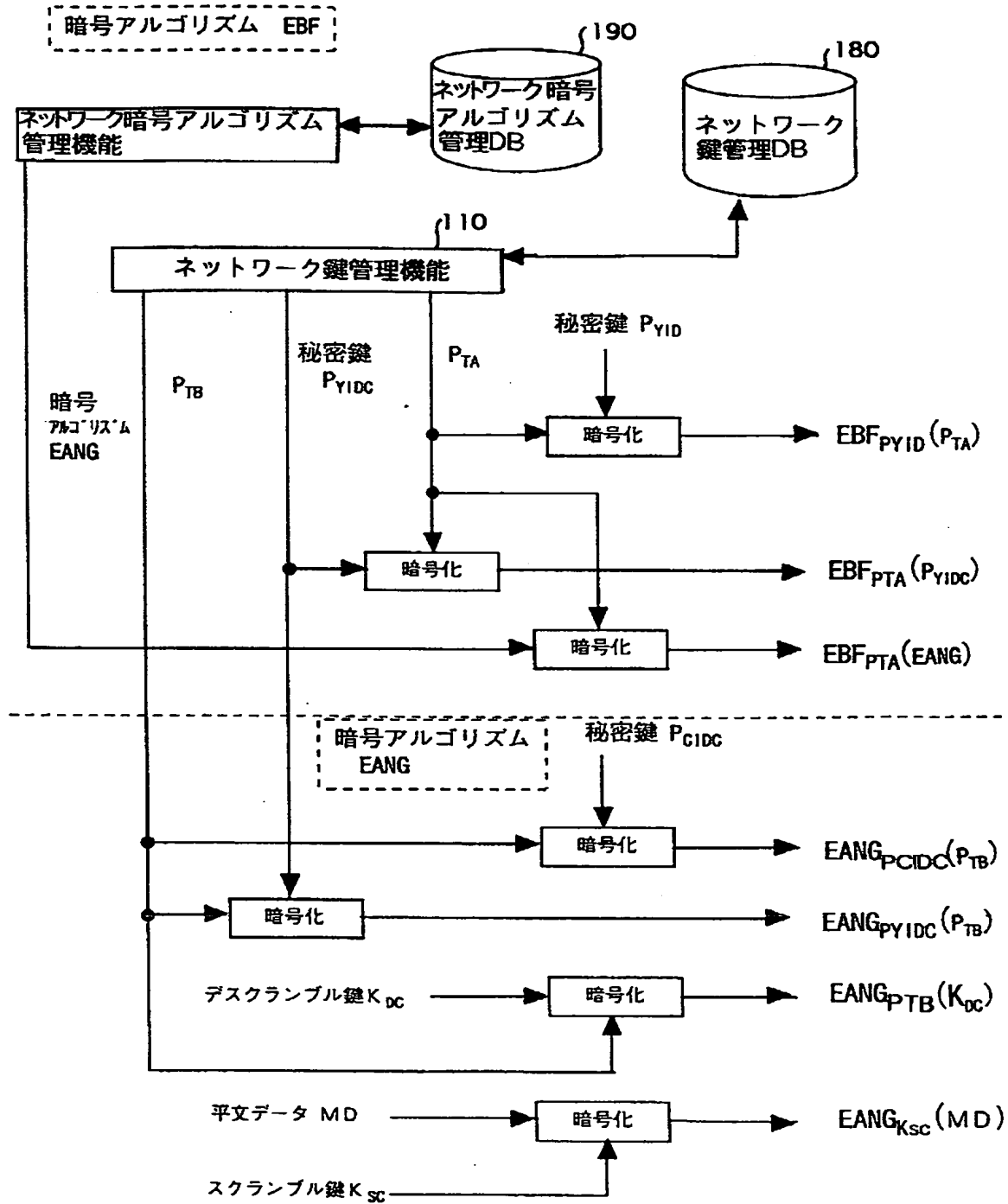
【図7】

図7 (共通鍵暗号による暗号化通信)



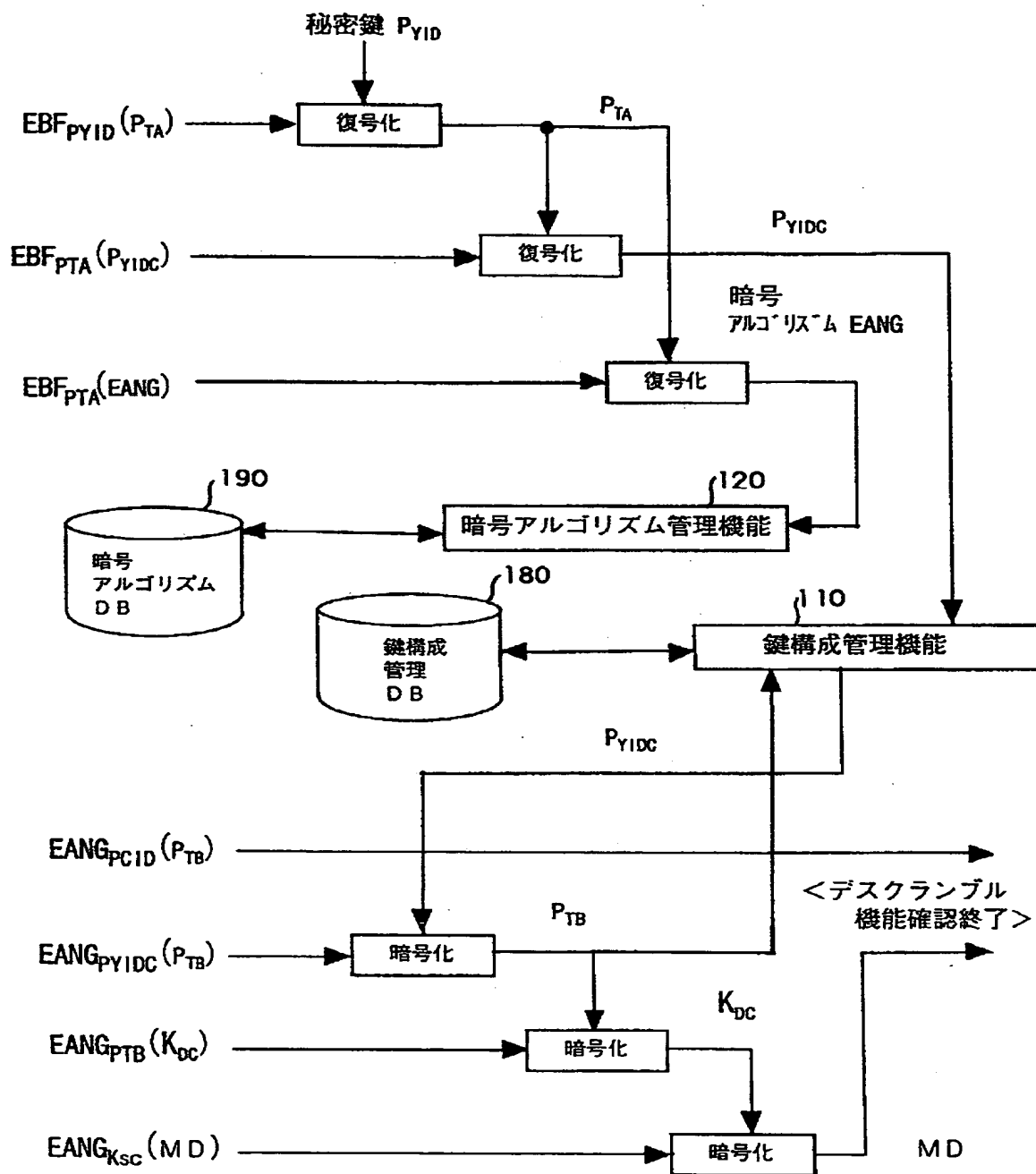
【図 8】

図 8



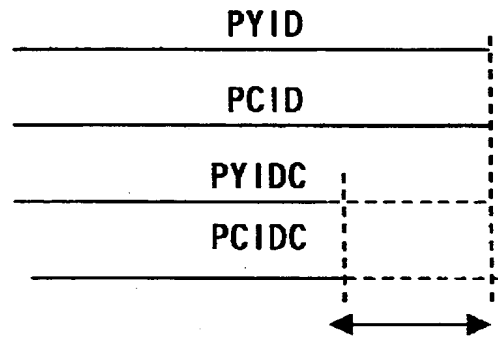
【図9】

図9



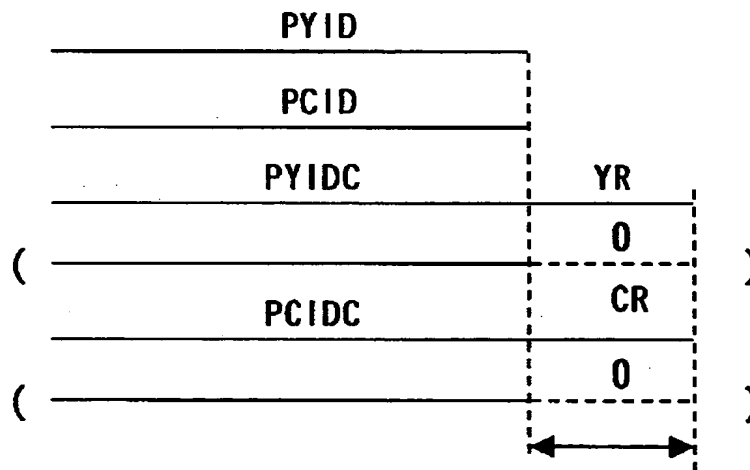
【図 10】

図 10



削除する鍵長

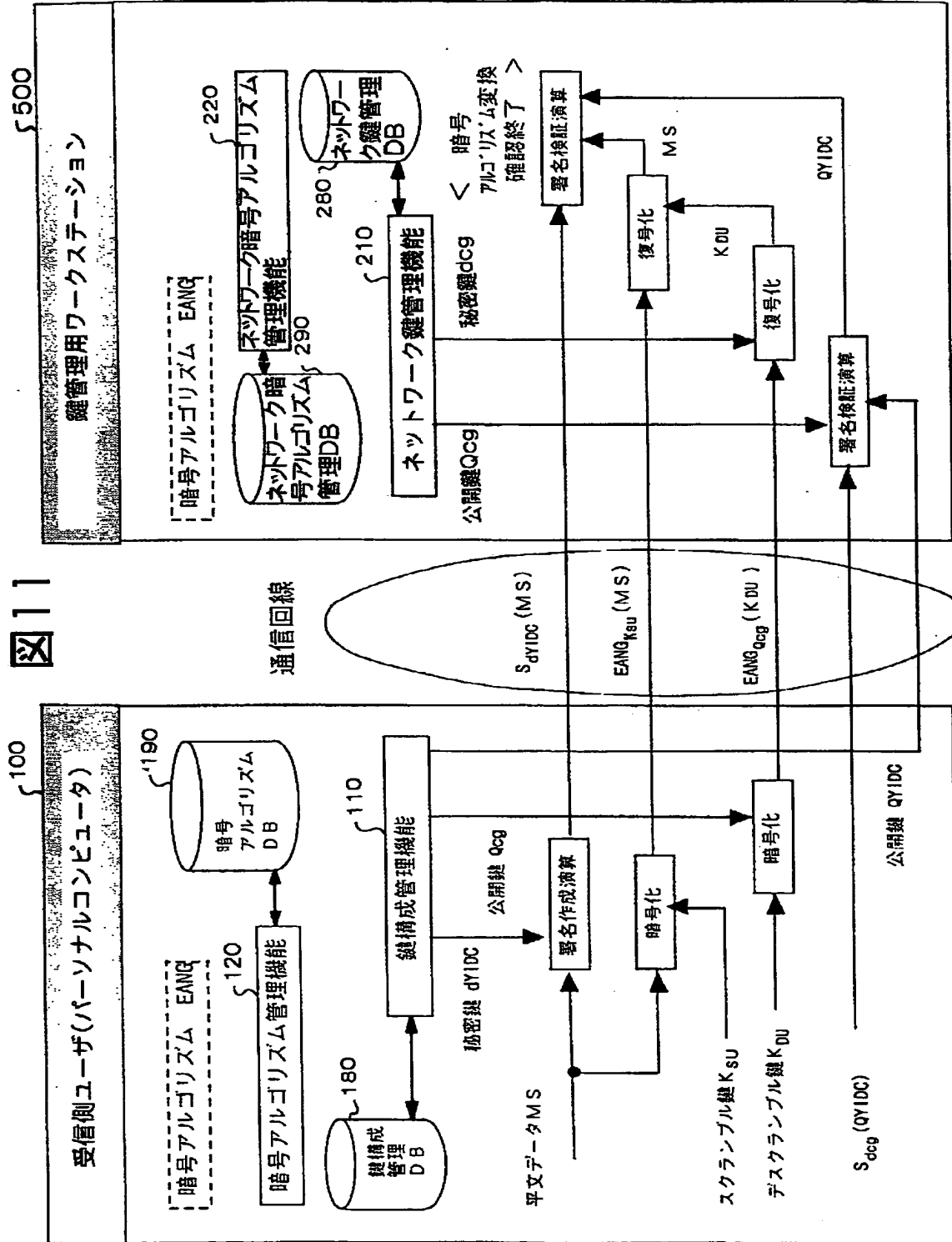
(a) 鍵長が短くなる場合



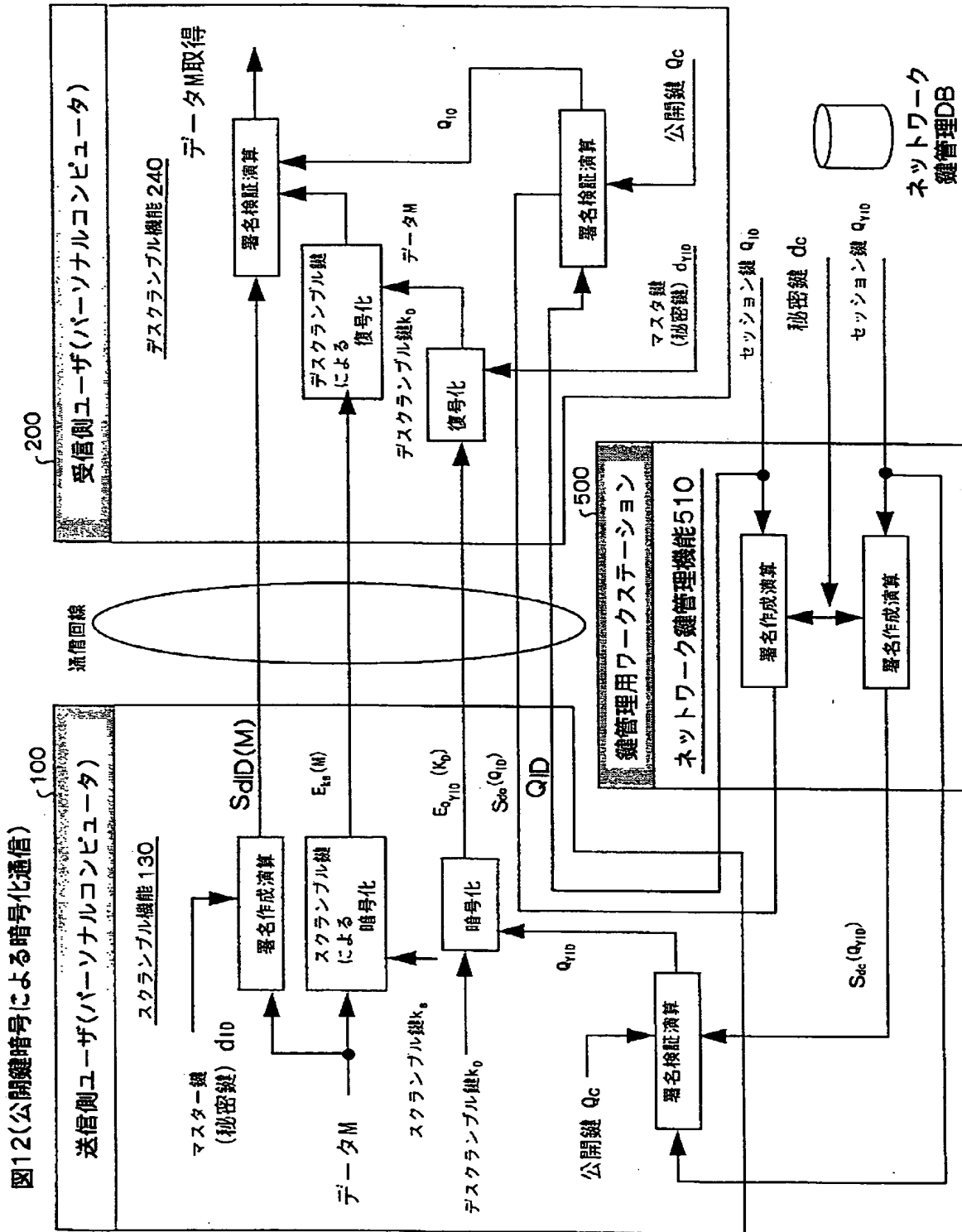
追加する鍵長

(b) 鍵長が長くなる場合

【図11】

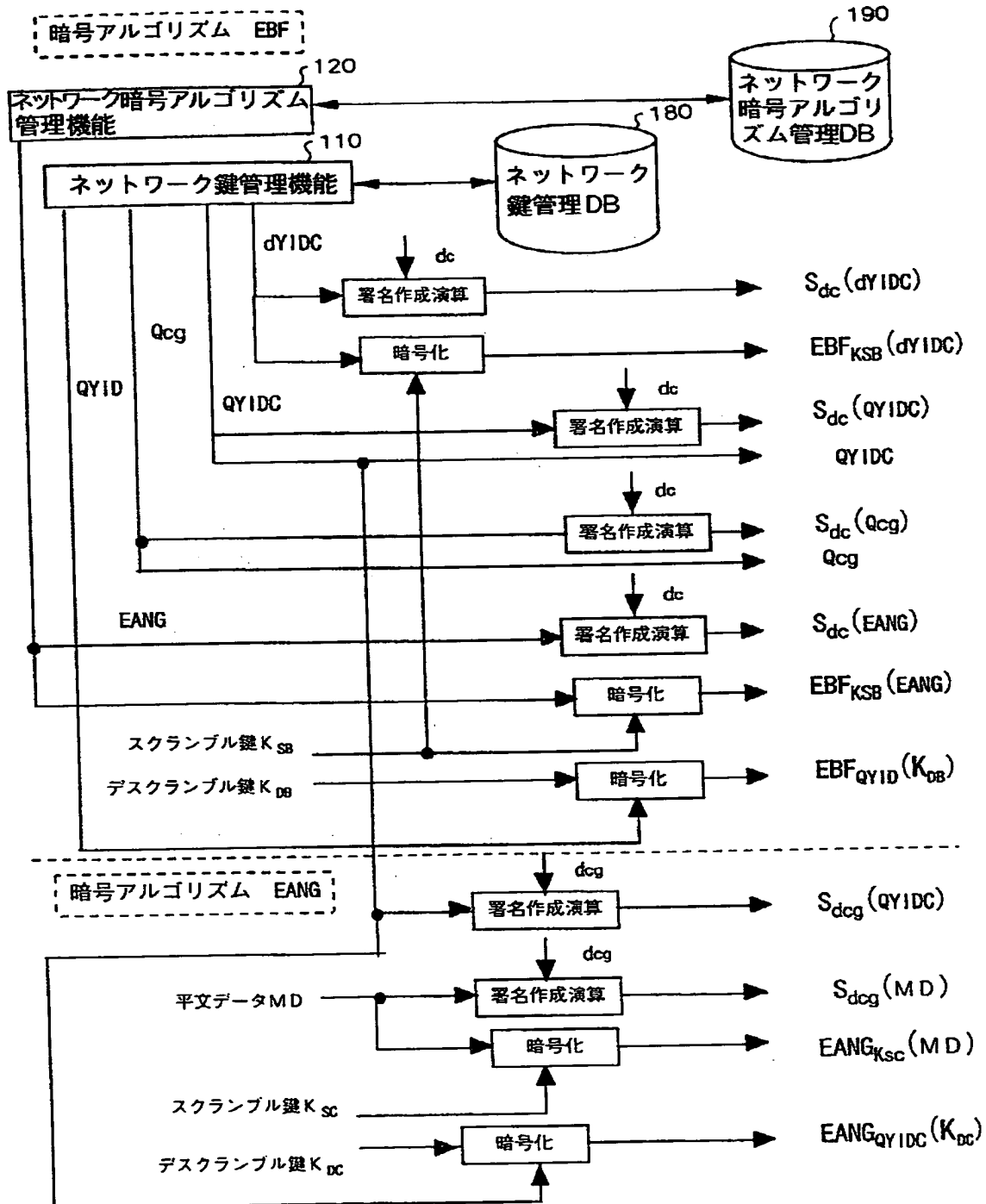


【図12】



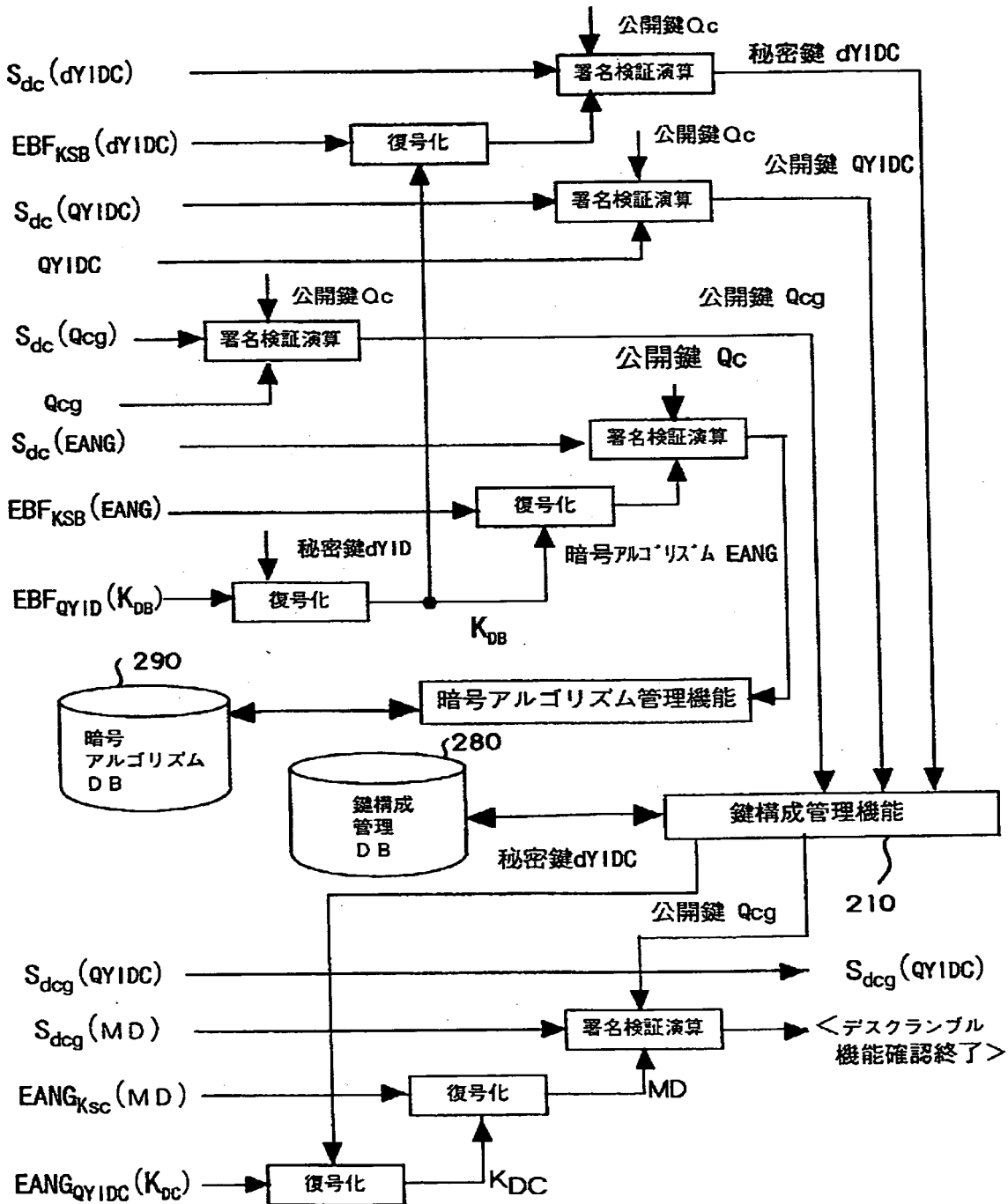
【図 13】

図 13

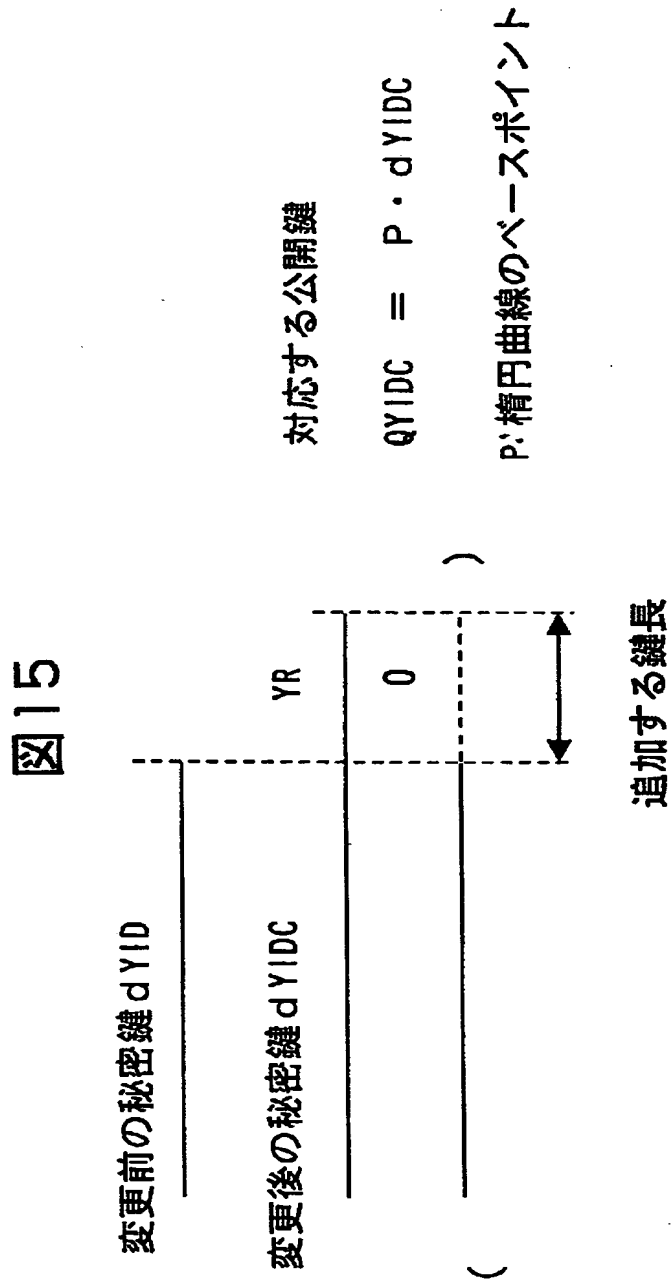


【図 14】

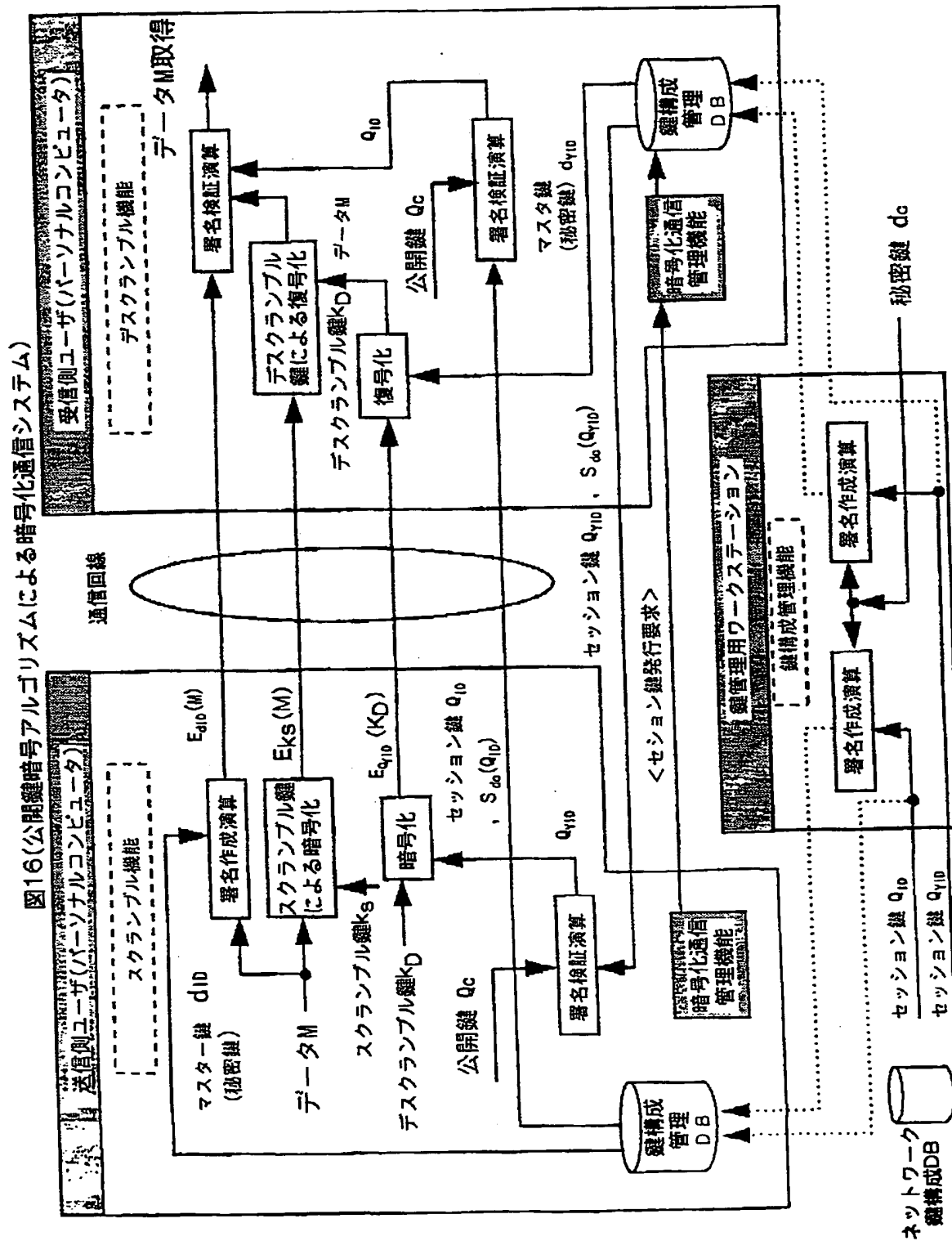
図 14



【図 15】

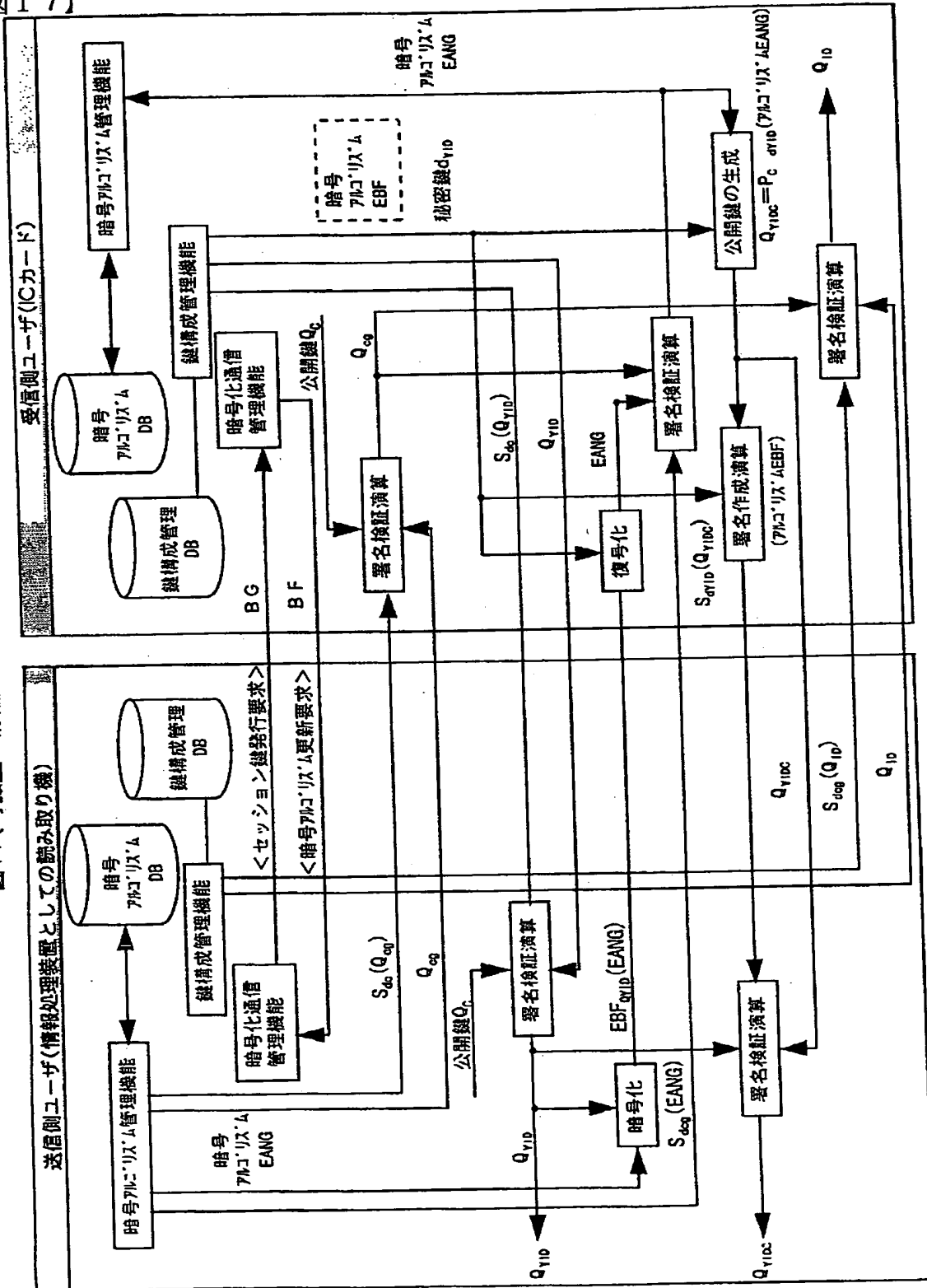


【図 16】

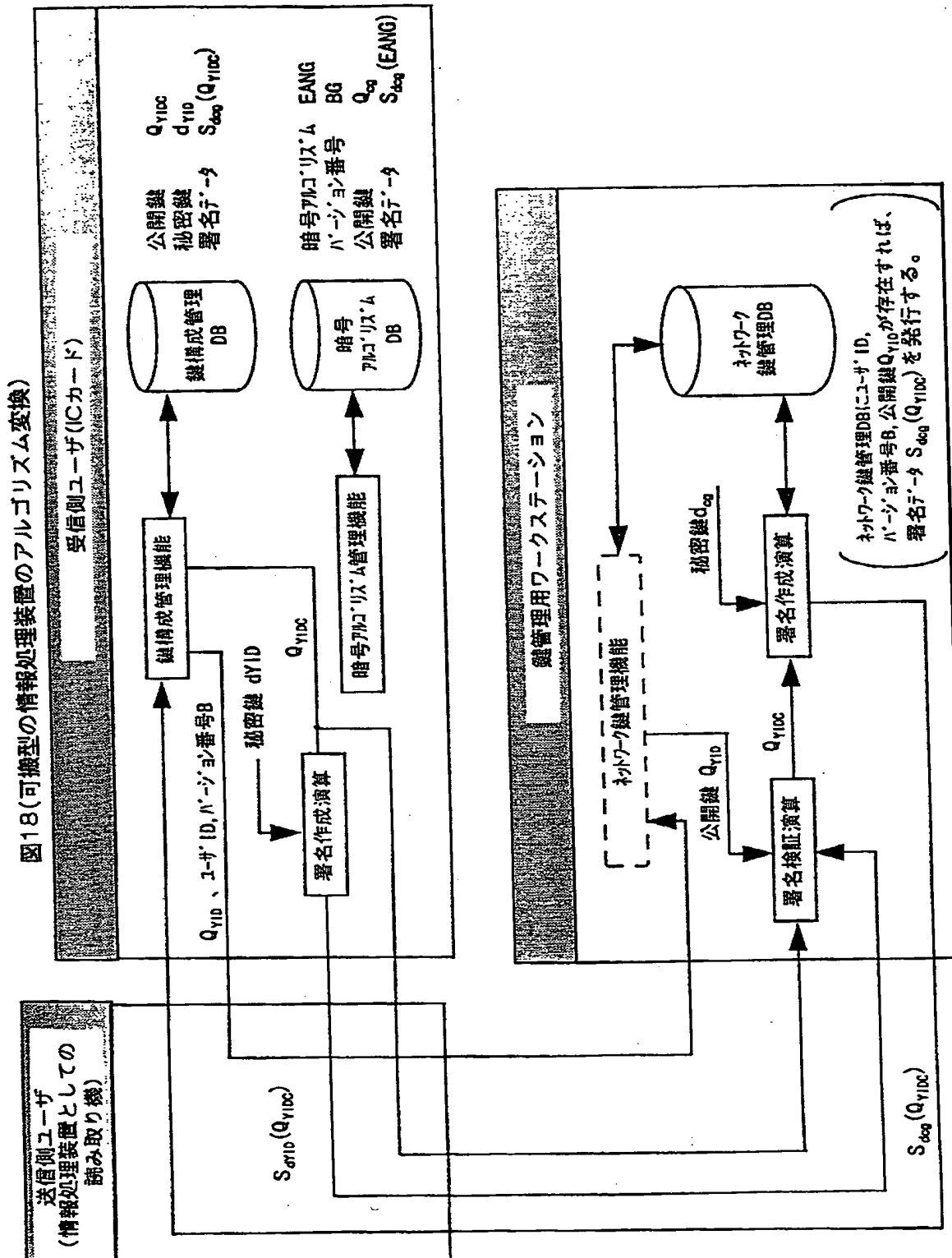


【図 17】

図17(可搬型の情報処理装置のアルゴリズム変換)

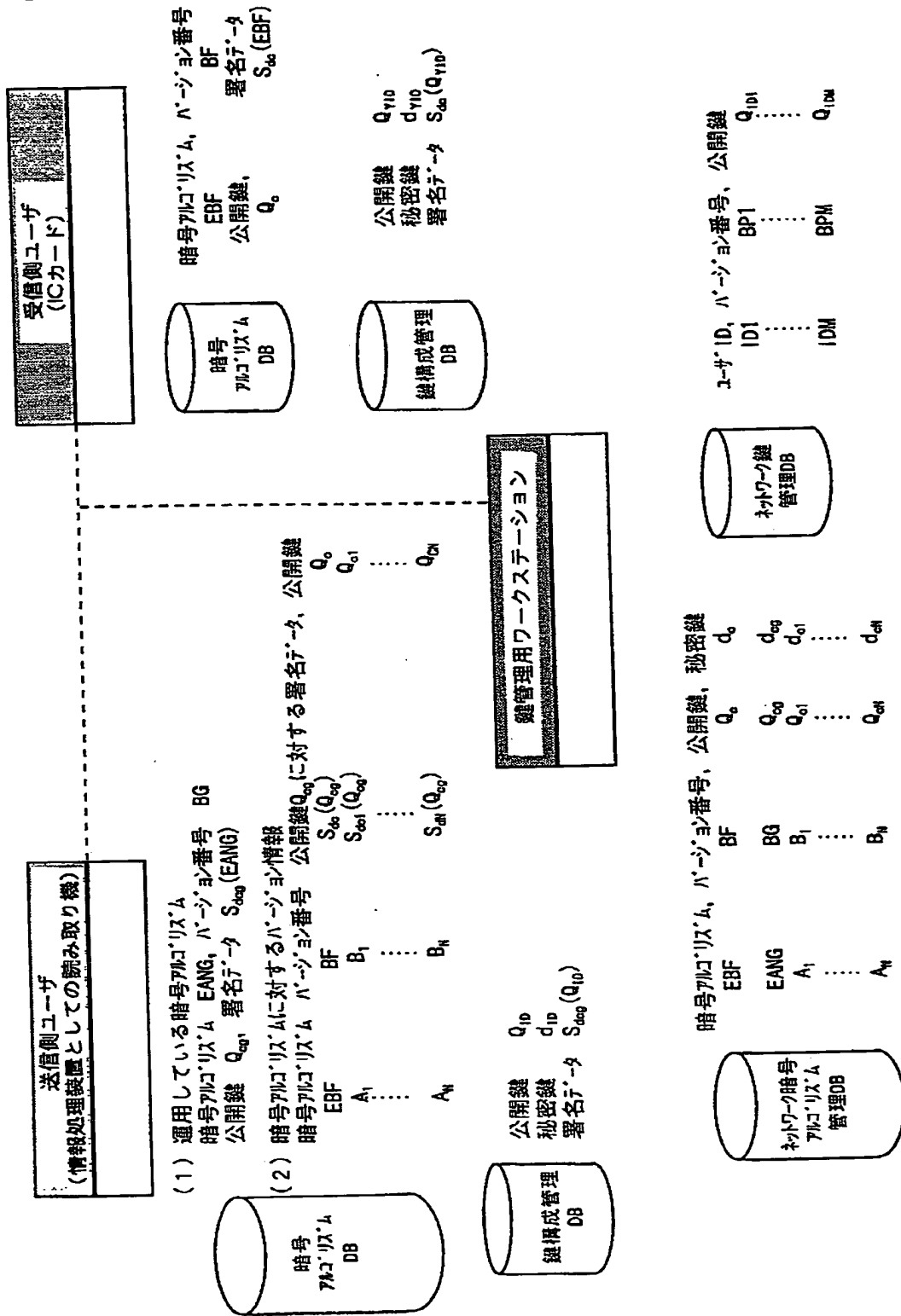


【图 18】

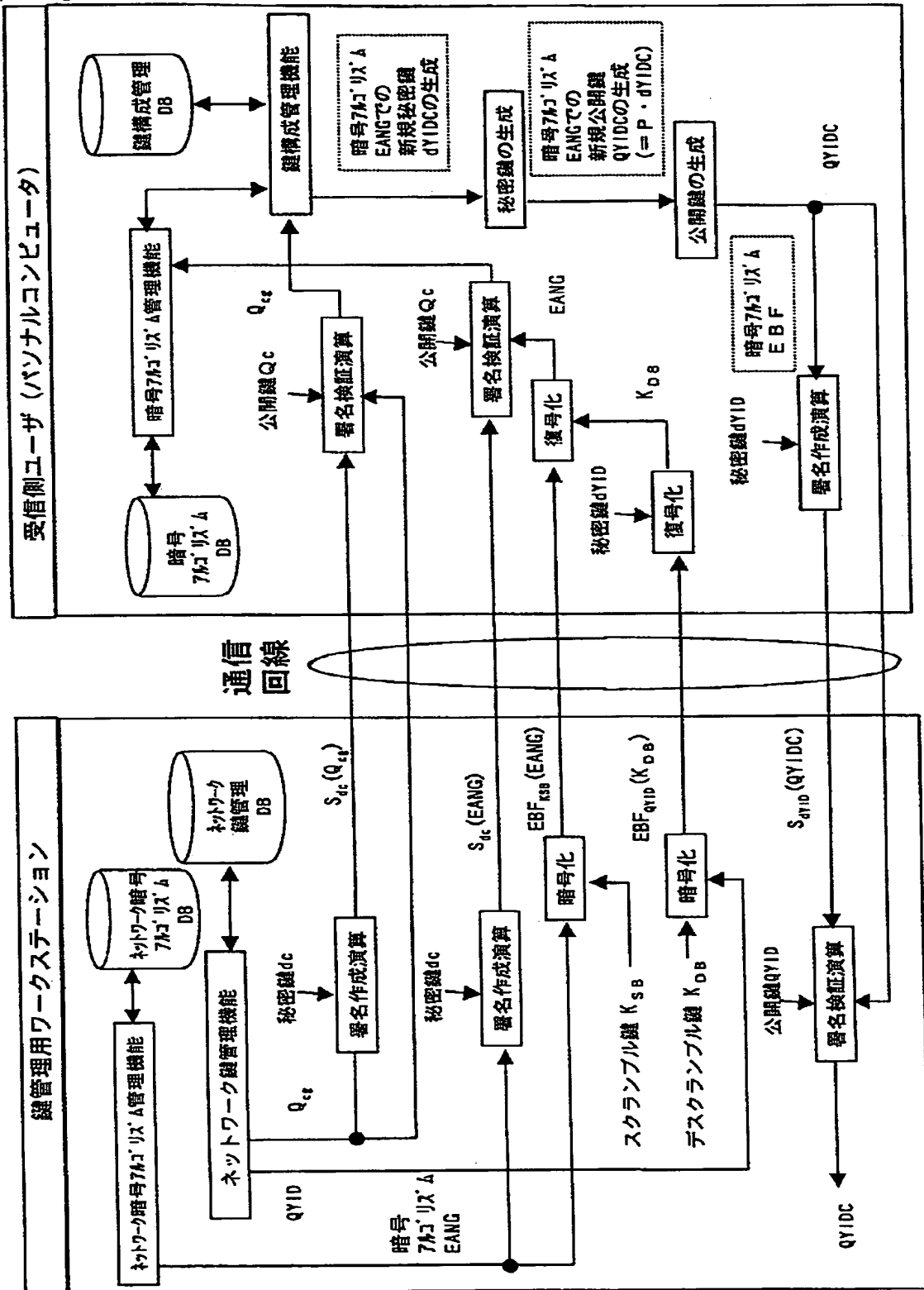
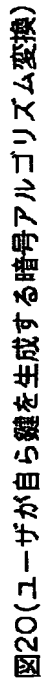


【図 19】

図19(鍵と暗号アルゴリズムに関するDB)

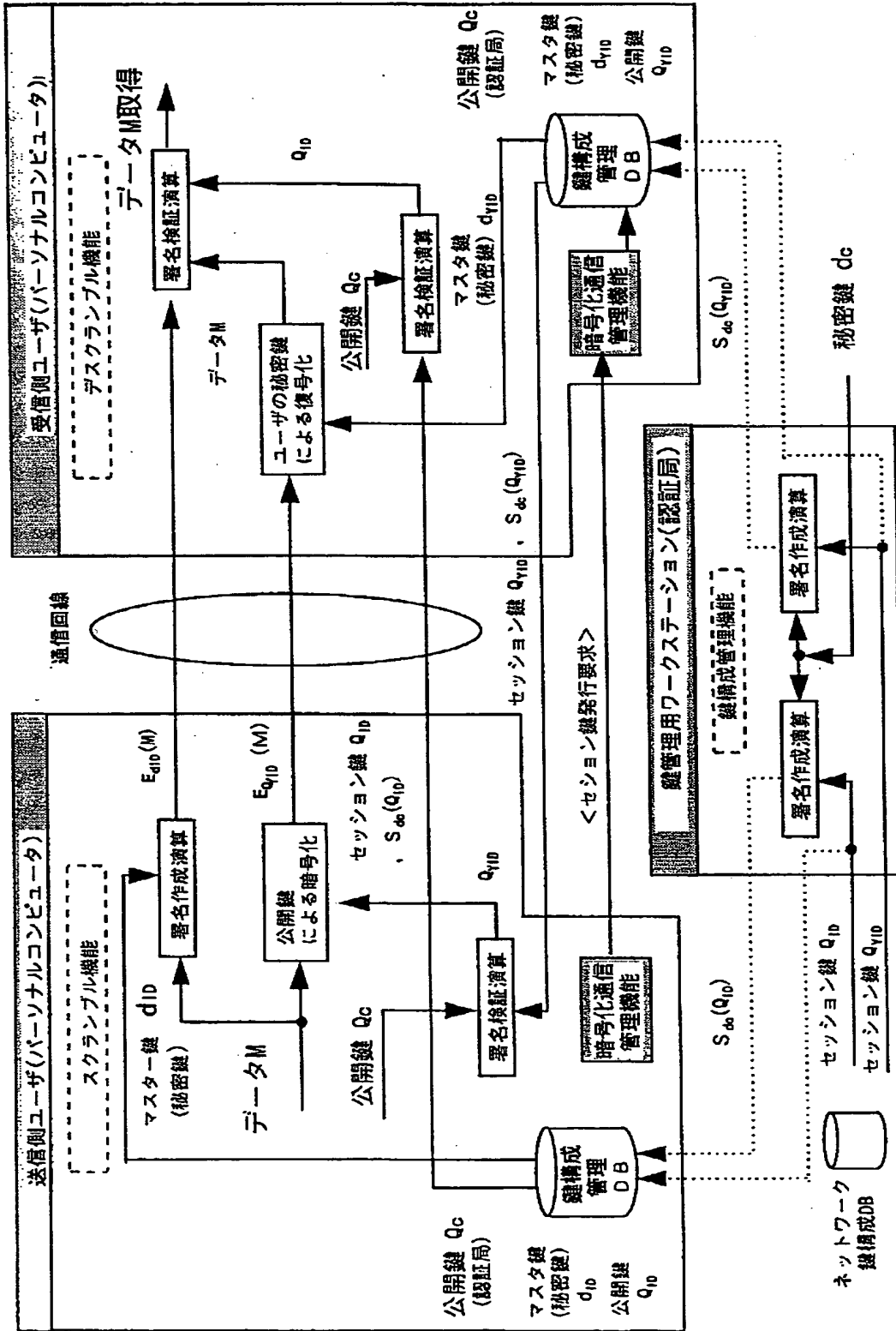


【図 20】



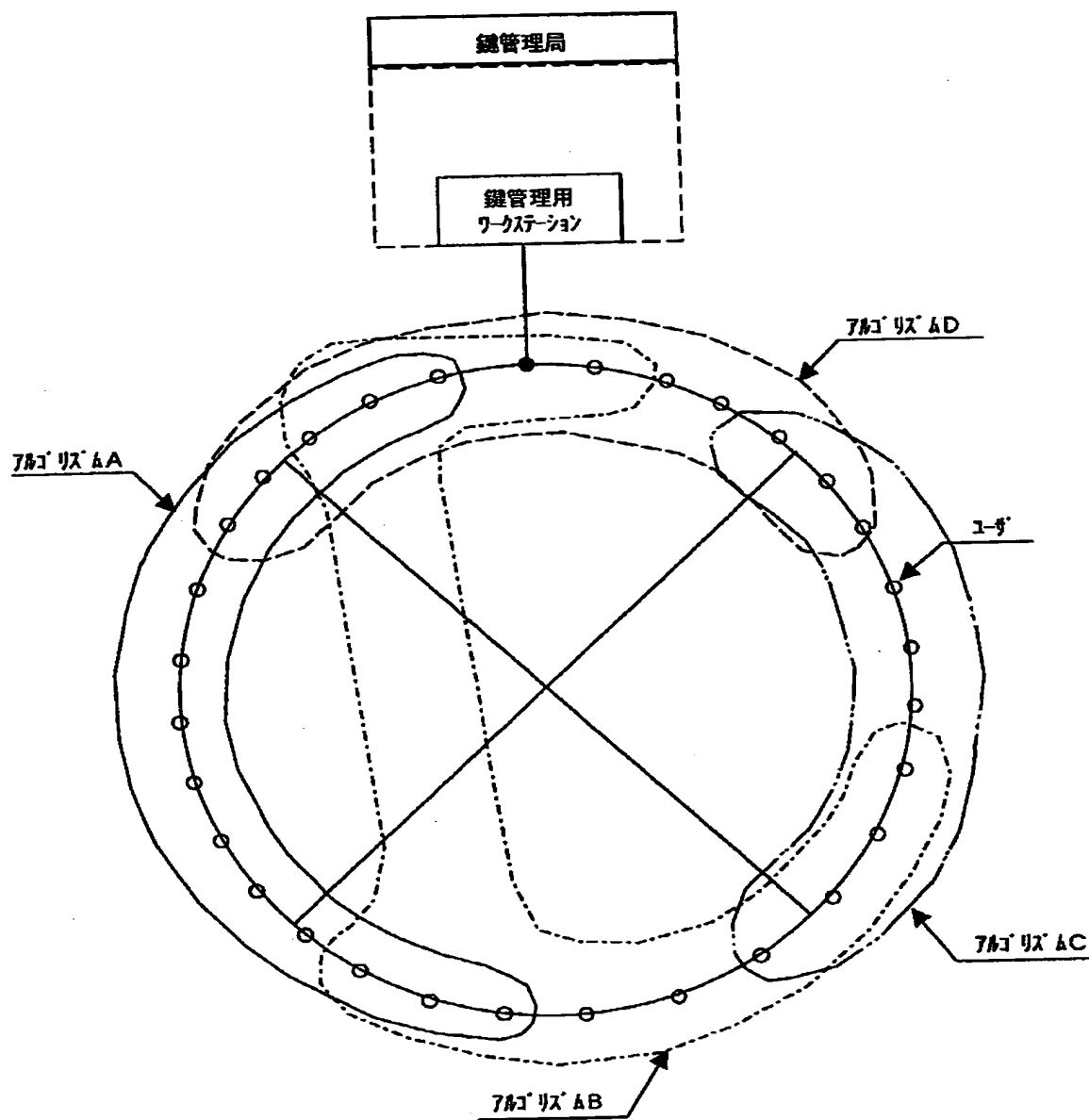
【図 21】

図21 (公開鍵暗号アルゴリズムによる暗号化通信システム)

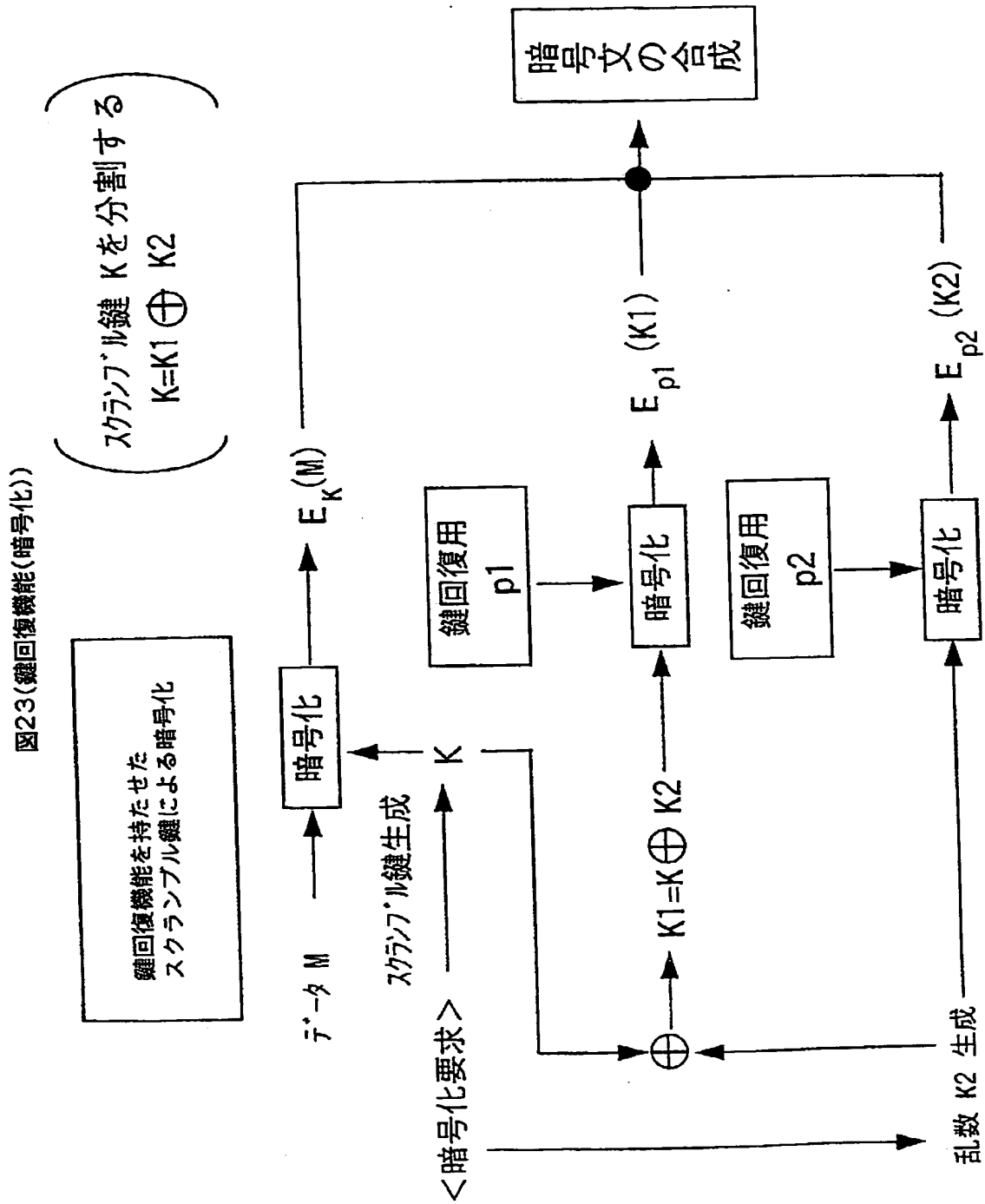


【図 22】

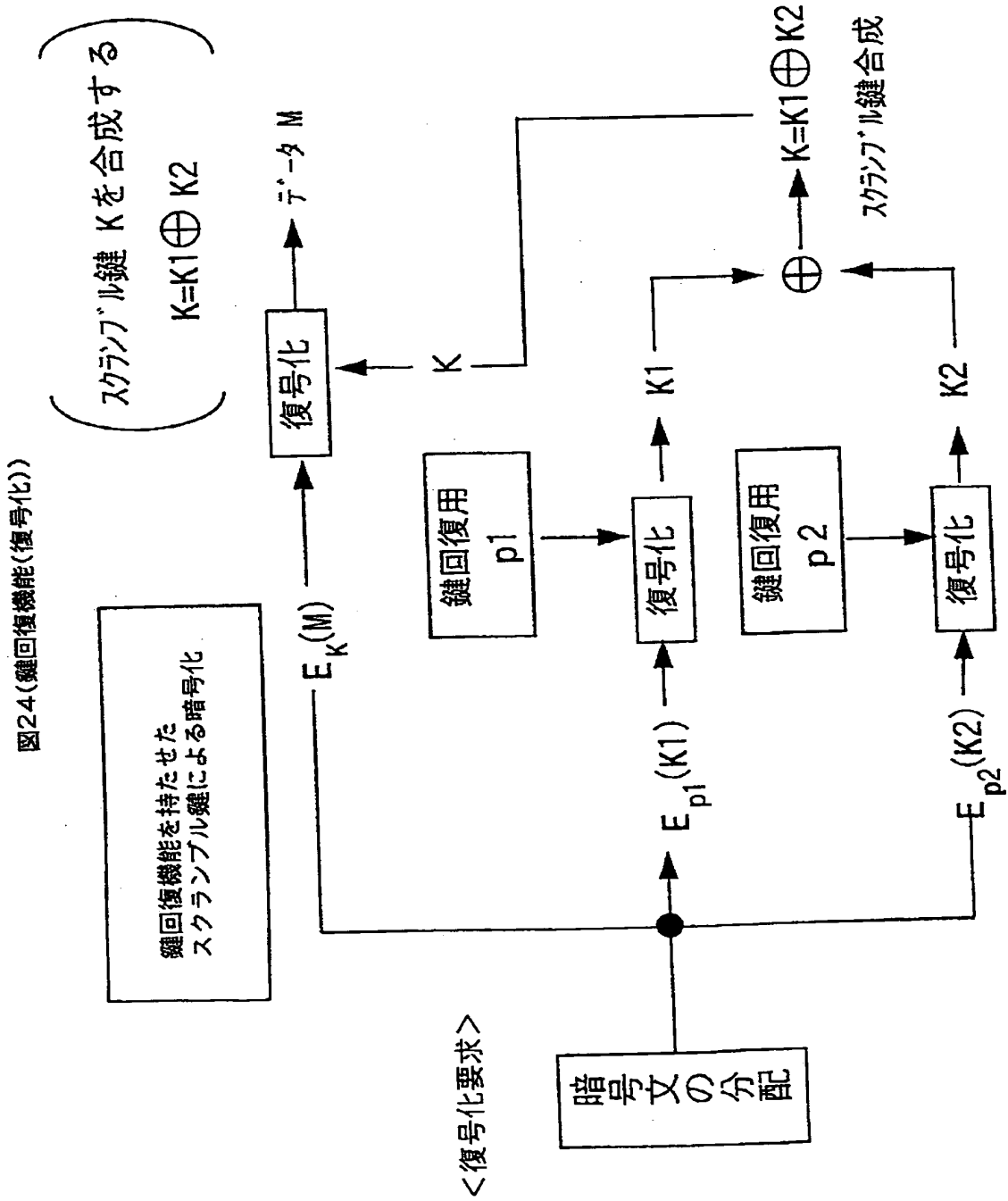
図22(複数の暗号アルゴリズムの存在するネットワーク通信システム)



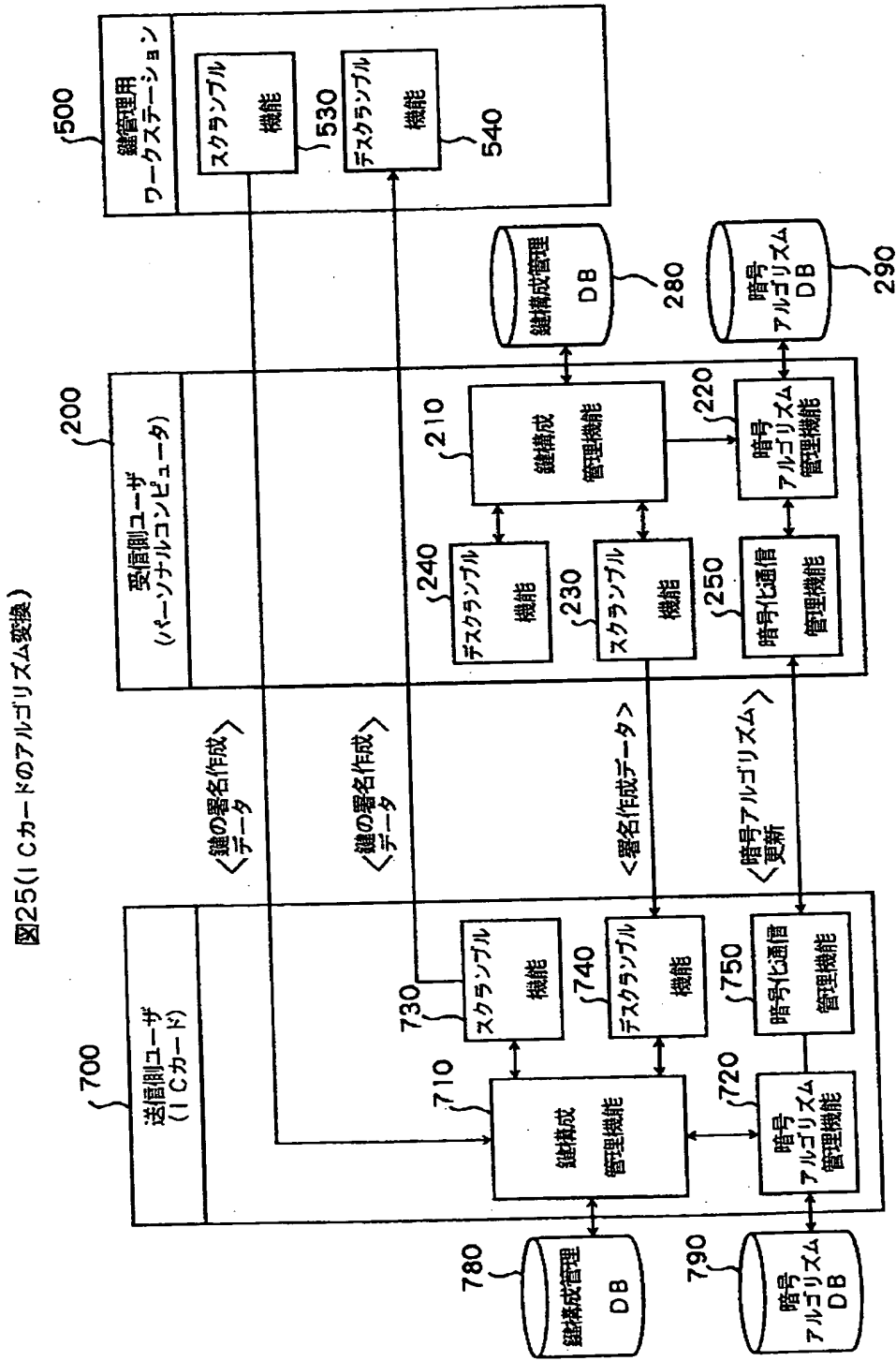
【図 23】



【図 24】



【図 25】



【書類名】 要約書

【要約】

【課題】 運用する暗号アルゴリズムを別の暗号アルゴリズムに変換する。

【解決手段】 グループAに属するユーザが使用するパーソナルコンピュータ100、及び、グループBに属するユーザが使用するパーソナルコンピュータ200で相異なる暗号アルゴリズムが運用されるとき、パーソナルコンピュータ100において、パーソナルコンピュータ200で運用される暗号アルゴリズムを、パーソナルコンピュータ200で運用される暗号アルゴリズムで暗号化してパーソナルコンピュータ200に伝送する。

【選択図】 図1

【書類名】
【訂正書類】

職権訂正データ
特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】

000005108

【住所又は居所】

東京都千代田区神田駿河台四丁目6番地

【氏名又は名称】

株式会社日立製作所

【特許出願人】

【識別番号】

000153421

【住所又は居所】

神奈川県横浜市戸塚区戸塚町216番地

【氏名又は名称】

株式会社日立アドバンスシステムズ

【特許出願人】

【識別番号】

000233217

【住所又は居所】

千葉県習志野市東習志野7丁目1番1号

【氏名又は名称】

日立京葉エンジニアリング株式会社

【代理人】

申請人

【識別番号】

100087170

【住所又は居所】

神奈川県横浜市西区北幸2丁目9番10号 横浜H

Sビル7階

【氏名又は名称】

富田 和子

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号

[000153421]

1. 変更年月日

1990年 8月 8日

[変更理由]

新規登録

住 所

神奈川県横浜市戸塚区戸塚町216番地

氏 名

株式会社日立アドバンスシステムズ

出 願 人 履 歴 情 報

識別番号

[000233217]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

千葉県習志野市東習志野7丁目1番1号

氏 名

日立京葉エンジニアリング株式会社